ProtectTools

ユーザ ガイド

本書の内容は、将来予告なしに変更されることがあります。HP 製品およびサービスに関する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。

初版 2007 年 1 月

製品番号：438371-291

目次

1 セキュリティの概要

2 Credential Manager for HP ProtectTools

3 Embedded Security for HP ProtectTools

4 Java Card Security for HP ProtectTools

1 セキュリティの概要

HP ProtectTools セキュリティ マネージャ ソフトウェアは、コンピュータ本体、ネットワーク、および重要なデータを不正なアクセスから保護するために役立つセキュリティ機能を提供します。 以下のソフトウェア モジュールによって、高度なセキュリティ機能が提供されます。

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Device Access Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools

コンピュータで利用可能なソフトウェア モジュールは、モデルによって異なる可能性があります。たとえば、Embedded Security for HP ProtectTools は、TPM（Trusted Platform Module）セキュリティ チップが内蔵されているコンピュータでのみ使用できます。

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。 詳しくは、http://www.hp.com/jp/にアクセスしてください。

注記： このガイドの操作手順は、該当する HP ProtectTools ソフトウェア モジュールがすでにインストールされていることを前提に書かれています。

HP ProtectTools の機能

次の表で、HP ProtectTools モジュールの主な機能を詳しく説明します。

モジュール	主な機能
Credential Manager for HP ProtectTools	● Credential Manager には、個人のパスワードを保管できます ● シングルサインオンは、パスワードで保護されたさまざまな Web サイト、アプリケーション、およびネットワーク リソース用の複数のパスワードを記憶します ● シングルサインオンは、ユーザ認証に Java™カードや指紋認証などの異なるセキュリティ テクノロジの組み合わせを要求することによって、さらなる保護機能を提供します ● パスワード記憶域は暗号化によって保護されており、TPM 内蔵セキュリティ チップ、または Java カードや指紋認証などのセキュリティ デバイス認証を使用することによって強化できます
Embedded Security for HP ProtectTools	● Embedded Security は、TPM（Trusted Platform Module）内蔵セキュリティ チップを使用して、コンピュータ本体に保存されている機密のユーザ データまたは証明情報を不正なアクセスから保護するために役立ちます ● Embedded Security を使用すると、ユーザ データを保護するための PSD（Personal Secure Drive）を作成できます ● Embedded Security は、保護されたデジタル証明情報の操作のための他社製のアプリケーション（Microsoft Outlook や Internet Explorer など）をサポートします
Java Card Security for HP ProtectTools	● Java Card Security は、オペレーティング システムがロードされる前のユーザ認証を行うために、HP ProtectTools Java Card を設定します ● Java Card Security では、管理者とユーザの Java Card を個別に設定します
BIOS Configuration for HP ProtectTools	● BIOS Configuration を使用すると、電源投入時のユーザおよび管理者パスワードの管理機能にアクセスできます ● BIOS Configuration は、f10 セットアップと呼ばれる、ブート前 BIOS コンフィギュレーション ユーティリティの代わりに使用できます ● 内蔵セキュリティ チップで機能強化された DriveLock は、ハードドライブがシステムから取り外されている場合でも、ハードドライブを不正なアクセスから保護するために役立ちます。ユーザは、内蔵セキュリティ チップのユーザ パスワード以外のパスワードを記憶する必要がありません

モジュール	主な機能
Device Access Manager for HP ProtectTools	● Device Access Manager を使用すると、IT 管理者は、ユーザ プロファイルに基づいてデバイスへのアクセスを制御できます ● Device Access Manager は、不正なユーザが外部のストレージメディアを使用してデータを削除したり、外部のメディアからシステムにウィルスを侵入させたりできないようにします ● 管理者は、特定の個人またはユーザのグループに対して、書き込み可能なデバイスへのアクセスを無効にすることができます
Drive Encryption for HP ProtectTools	● Drive Encryption では、ボリューム全体にわたる完全なハードドライブ暗号化が可能です ● Drive Encryption では、データの暗号化解除やデータへのアクセスにブート前認証が強制されます

HP ProtectTools セキュリティへのアクセス

Windows®の[コントロール パネル]から HP ProtectTools セキュリティにアクセスするには、次の操作を行います。

▲ **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

注記： Credential Manager モジュールを設定した後は、Windows のログオン画面から直接 Credential Manager にログオンして HP ProtectTools を起動することもできます。 詳しくは、20 ページの 「Credential Manager を使用した Windows へのログオン」を参照してください。

主なセキュリティの目的の実現

各 HP ProtectTools モジュールが連携して動作することにより、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題に対処するためのソリューションを提供できます。

- 盗難からの保護
- 機密データへのアクセス制限
- 内部または外部からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成

盗難からの保護

盗難の例として、空港の検問所での、機密データや顧客情報を含むコンピュータの盗難が挙げられます。 盗難からの保護には、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。 以下の項目を参照してください。
  - 53 ページの 「スマート カードの電源投入時認証サポートの有効/無効の設定」
  - 54 ページの 「内蔵セキュリティの電源投入時認証サポートの有効/無効の設定」
  - 46 ページの 「Java Card への名前の割り当て」
  - 65 ページの 「Drive Encryption for HP ProtectTools」
- DriveLock（ドライブロック）は、ハードドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。 55 ページの 「自動 DriveLock によるハードドライブのプロテクトの有効/無効の設定」を参照してください。
- Embedded Security for HP ProtectTools モジュールで提供される Personal Secure Drive 機能では、機密データを暗号化して、認証なしではアクセスできないようにします。 以下の項目を参照してください。
  - 34 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
  - 37 ページの 「Personal Secure Drive（PSD）の使用」

機密データへのアクセス制限

契約検査官がオンサイトで作業しており、機密の財務データの確認のためにコンピュータへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。 データへのアクセスを制限するには、以下の機能が役立ちます。

- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報を印刷したり、ハードドライブからリムーバブル メディアにコピーしたりできないように、書き込み可能なデバイスへのアクセスを制限することができます。 62 ページの 「デバイス クラス構成（詳細設定）」を参照してください。
- DriveLock は、ハードドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。 55 ページの 「自動 DriveLock によるハードドライブのプロテクトの有効/無効の設定」を参照してください。

内部または外部からの不正なアクセスの防止

機密データや顧客情報を含むコンピュータが内部または外部からアクセスされると、不正なユーザが社内ネットワーク リソースに侵入したり、金融サービス、役員、または研究開発チームからのデータ、または患者記録や個人の財務データなどの個人情報を入手したりできてしまう可能性があります。 不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。 以下の項目を参照してください。
  - 53 ページの 「スマート カードの電源投入時認証サポートの有効/無効の設定」
  - 54 ページの 「内蔵セキュリティの電源投入時認証サポートの有効/無効の設定」
  - 46 ページの 「Java Card への名前の割り当て」
  - 65 ページの 「Drive Encryption for HP ProtectTools」
- Embedded Security for HP ProtectTools は、以下の方法で、コンピュータ本体に保存されている機密のユーザ データまたは証明情報を保護するために役立ちます。
  - 34 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
  - 37 ページの 「Personal Secure Drive（PSD）の使用」
- Credential Manager for HP ProtectTools は、以下方法で、不正なユーザがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにするために役立ちます。
  - 14 ページの 「セットアップ手順」（Credential Manager のセットアップ）
  - 21 ページの 「シングルサインオンの使用」
- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報をハードドライブからコピーできないように、書き込み可能なデバイスへのアクセスを制限することができます。 61 ページの 「簡易構成」を参照してください。
- Personal Secure Drive 機能では、以下の方法で機密データを暗号化し、認証なしではアクセスできないようにします。
  - 34 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
  - 37 ページの 「Personal Secure Drive（PSD）の使用」

強力なパスワード ポリシーの作成

いくつもの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシーを使用する必要が生じた場合、Credential Manager for HP ProtectTools で以下の方法により、パスワードやシングルサインオンのための保護されたリポジトリが提供されます。

- 14 ページの 「セットアップ手順」（Credential Manager のセットアップ）
- 21 ページの 「シングルサインオンの使用」

セキュリティを強化するために、Embedded Security for HP ProtectTools は次に、ユーザ名とパスワードのリポジトリを保護します。 これにより、ユーザはメモに残したり覚えたりしなくても、複数の強力なパスワードを保持することができます。 34 ページの 「セットアップ手順」（Embedded Security のセットアップ）を参照してください。

その他のセキュリティ対策

セキュリティの役割の割り当て

コンピュータのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザに割り当てることが、重要な作業の 1 つです。

注記： 小さな組織や個人で使用する場合などは、一人の人がすべての役割を受け持つこともできます。

HP ProtectTools では、セキュリティの責任および権限を以下のように分けられます。

- セキュリティ オフィサ：企業またはネットワークのセキュリティ レベルを定義し、Java™ Cards、指紋認証システム、USB トークンなど、配備するセキュリティ機能を決定します。

  注記： HP ProtectTools の機能の多くは、セキュリティ オフィサが HP と協力してカスタマイズできます。 詳しくは、HP の Web サイト http://www.hp.com/jp/を参照してください。

- IT 管理者：セキュリティ オフィサによって定義されたセキュリティ機能を適用し、管理します。 また、一部の機能を有効または無効にできます。 たとえば、セキュリティ オフィサが Java Card の配備を決定した場合、IT 管理者は Java Card の BIOS セキュリティ モードを有効にすることができます。
- ユーザ：セキュリティ機能を使用します。 たとえば、セキュリティ オフィサおよび IT 管理者がシステムで Java Card を有効にしている場合、ユーザは Java Card の PIN を設定し、そのカードを認証に使用できます。

HP ProtectTools のパスワードの管理

HP ProtectTools セキュリティ マネージャの機能のほとんどは、パスワードによってセキュリティ保護されています。 次の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者だけが設定して使用するパスワードも示されています。 その他のすべてのパスワードは、一般のユーザまたは管理者が設定できます。

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
Credential Manager のログオン パスワード	Credential Manager	このパスワードには、次の 2 つのオプションがあります • Windows にログオンした後、Credential Manager にアクセスするための別のログオンで使用できます • Windows ログオン プロセスの代わりに使用し、Windows と Credential Manager に同時にアクセスできます
Credential Manager リカバリ ファイルのパスワード	Credential Manager、IT 管理者が設定	Credential Manager リカバリ ファイルへのアクセスを保護します
基本ユーザ キーのパスワード	Embedded Security	安全な電子メール、ファイル、およびフォルダの暗号化など Embedded Security 機能へのアクセスに使用します。 電源投入時認

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
注記： 内蔵セキュリティ パスワードとも呼ばれます		証に使用すると、コンピュータの起動時や再起動時、またはハイバネーションからの復帰時にコンピュータのデータを保護します
緊急リカバリ トークンのパスワード 注記： 緊急リカバリ トークン キーのパスワードとも呼ばれます	Embedded Security、IT 管理者が設定	内蔵セキュリティ チップ用のバックアップ ファイルである緊急リカバリ トークンへのアクセスを保護します
所有者のパスワード	Embedded Security、IT 管理者が設定	システムと TPM チップを、Embedded Security のすべての所有者機能への不正なアクセスから保護します
Java™ Card の PIN	Java Card Security	Java Card の内容へのアクセスを保護し、Java Card のユーザを認証します。 電源投入時認証に使用すると、Java Card の PIN の入力により[Computer Setup]ユーティリティおよびコンピュータのデータも保護されます Java Card トークンが選択されている場合は、Drive Encryption のユーザを認証します
[Computer Setup]のパスワード 注記： BIOS の管理者パスワード、f10 セットアップ パスワード、またはセキュリティ セットアップ パスワードとも呼ばれます	BIOS Configuration、IT 管理者が設定	[Computer Setup]ユーティリティへのアクセスを保護します
Power-on Password（電源投入時パスワード）	BIOS Configuration	コンピュータの起動時や再起動時、またはハイバネーションからの復帰時にコンピュータのデータを保護します
Windows のログオン パスワード	Windows の[コントロール パネル]	手動ログオンで使用するか、または Java Card に保存できます

安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。 ただし一般的には、強力なパスワードを作成し、そのパスワードが危険にさらされないようにするために、以下のガイドラインを考慮してください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させます。
- 可能な場合は常に、半角アルファベットと半角数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。 たとえば、アルファベットの I または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分割します。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。 いくつかの文字や数字をその次の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピュータのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピュータ上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

HP ProtectTools Backup and Restore

HP ProtectTools Backup and Restore には、サポートされているすべての HP ProtectTools モジュールからの証明情報をバックアップおよび復元するための便利で、すばやく実行できる機能が用意されています。

証明情報および設定のバックアップ

以下の方法で証明情報をバックアップできます。

- [HP ProtectTools Backup Wizard]（HP ProtectTools バックアップ ウィザード）を使用して、HP ProtectTools モジュールの選択とバックアップを行う
- 事前に選択された HP ProtectTools モジュールをバックアップする

  注記： この方法を使用するには、バックアップ オプションを設定する必要があります。

- バックアップのスケジュールを設定する

  注記： この方法を使用するには、バックアップ オプションを設定する必要があります。

[HP ProtectTools Backup Wizard]を使用した HP ProtectTools モジュールの選択とバックアップ

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Backup Options]**（バックアップ オプション）をクリックします。 [HP ProtectTools Backup Wizard]（HP ProtectTools バックアップ ウィザード）が起動します。 画面の説明に沿って操作し、証明情報をバックアップします。

バックアップ オプションの設定

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Backup Options]**（バックアップ オプション）をクリックします。 [HP ProtectTools Backup Wizard]（HP ProtectTools バックアップ ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。
5. **[Storage File Password]**（ストレージ ファイルのパスワード）を設定および確認したら、**[Remember all passwords and authentication values for future automated backups]**（将来の自動バックアップのすべてのパスワードと認証値を記憶する）を選択します。
6. **[Save Settings]**（設定の保存）→**[Finish]**（完了）の順にクリックします。

事前に選択された HP ProtectTools モジュールのバックアップ

注記： この方法を使用するには、バックアップ オプションを設定する必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Backup]**をクリックします。

バックアップ スケジュールの設定

注記： この方法を使用するには、バックアップ オプションを設定する必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Schedule Backups]**（バックアップ スケジュールの設定）をクリックします。

4. **[Task]**（タスク）タブで、**[Enable]**（有効）チェック ボックスにチェックを入れて、スケジュールされたバックアップを有効にします。
5. **[Set Password]**（パスワードの設定）をクリックし、**[Set Password]**（パスワードの設定）ダイアログ ボックスでパスワードを入力して確認します。 **[OK]**をクリックします。
6. **[Apply]**（適用）をクリックします。 **[Schedule]**（スケジュール）タブをクリックします。 **[Schedule Task]**（タスクのスケジュール）の矢印をクリックし、自動バックアップの頻度を選択します。
7. **[Start time]**（開始時刻）の下で、**[Start time]**（開始時刻）の矢印を使用して、バックアップ開始の正確な時刻を選択します。
8. **[Advanced]**（詳細）をクリックして、開始日、終了日、および繰り返しタスクの設定を選択します。 **[Apply]**（適用）をクリックします。
9. **[Settings]**（設定）をクリックし、**[Scheduled Task Completed]**（スケジュールされたタスクの完了）、**[Idle Time]**（アイドル時間）、および**[Power Management]**（電源管理）の設定を選択します。
10. **[Apply]**（適用）をクリックし、**[OK]**をクリックしてダイアログ ボックスを閉じます。

証明情報の復元

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Restore]**（復元）をクリックします。 [HP ProtectTools Restore Wizard]（HP ProtectTools 復元ウィザード）が起動します。 画面に表示される説明に沿って操作します。

設定の選択

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、設定を選択して**[OK]**をクリックします。

2 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools では、次のセキュリティ機能を使用して、コンピュータを不正なアクセスから保護します。

- Windows へのログオン時のパスワードに代わる、Java Card や指紋認証システムなどを使用した Windows へのログオン。 詳しくは、15 ページの 「証明情報の登録」を参照してください。
- Web サイト、アプリケーション、および保護されたネットワーク リソースでの証明情報を自動的に記憶するシングルサインオン機能。
- Java Card や指紋認証システムなどの、オプションのセキュリティ デバイスのサポート。
- コンピュータのロック解除にはオプションのセキュリティ デバイスを使用した認証を必要とするなどの、追加のセキュリティ設定のサポート。

セットアップ手順

Credential Manager へのログオン

設定に応じて、以下のどれかの方法で Credential Manager にログオンできます。

- [Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）（推奨）
- 通知領域の[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコン
- HP ProtectTools セキュリティ マネージャ

注記： Windows のログオン画面の Credential Manager ログオン入力領域から Credential Manager にログオンすると、同時に Windows にもログオンします。

最初に Credential Manager を起動するときは、通常の Windows ログオン パスワードでログオンします。 その後、Credential Manager アカウントが、Windows のログオン証明情報を使用して自動的に作成されます。

Credential Manager にログオンした後、指紋や Java Card などの追加の証明情報を登録できます。 詳しくは、15 ページの 「証明情報の登録」を参照してください。

次回のログオン時には、ログオン ポリシーを選択して、登録された証明情報の任意の組み合わせを使用することができます。

[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）の使用

[Credential Manager Logon Wizard]を使用して Credential Manager にログオンするには、以下の手順で操作します。

1. 以下のどれかの方法で[Credential Manager Logon Wizard]を起動します。
   - Windows のログオン画面を使用する
   - 通知領域から、**[HP ProtectTools Security Manager]**アイコンをダブルクリックする
   - ProtectTools セキュリティ マネージャの[Credential Manager]（証明情報マネージャ）ページから、ウィンドウの右上隅にある**[Log On]**（ログオン）リンクをクリックする
2. 画面の説明に沿って操作し、Credential Manager にログオンします。

最初のログオン

開始する前に、管理者アカウントで Windows にログオンし、Credential Manager にログオンしていないことが必要です。

1. 通知領域内の[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコンをダブルクリックして、HP ProtectTools セキュリティ マネージャを起動します。 [HP ProtectTools Security Manager]ウィンドウが開きます。
2. 左側のパネルで**[Credential Manager]**（証明情報マネージャ）をクリックしてから、右側のパネルの右上隅にある**[Log On]**（ログオン）をクリックします。 [Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）が起動します。
3. **[Password]**（パスワード）ボックスに Windows パスワードを入力して**[Next]**（次へ）をクリックします。

証明情報の登録

[My Identity]（個人 ID）ページを使用して、各種の認証方法、または証明情報を登録できます。 登録が完了した後、それらの方法を使用して Credential Manager にログオンできます。

指紋の登録

指紋認証システムでは、Windows パスワードではなく、指紋を使用して認証することで Windows にログオンできます。

指紋認証システムのセットアップ

1. Credential Manager にログオンしたら、指紋認証システムの指紋読み取り装置に指を押し当てます。 [Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。
2. 画面の説明に沿って操作し、指紋の登録と指紋認証システムのセットアップを完了します。
3. 別の Windows ユーザ用の指紋を登録するには、そのユーザとして Windows にログオンして手順 1 と 2 を繰り返します。

登録された指紋を使用した Windows へのログオン

1. 指紋を登録したらすぐに Windows を再起動します。
2. Windows の[ようこそ]画面で、登録された指のどれかを押し当てて Windows にログオンします。

Java Card、USB eToken、または仮想トークンの登録

注記： この手順を実行するには、カード リーダーを設定しておく必要があります。 リーダーが装備されていない場合は、18 ページの 「仮想トークンの作成」の説明に沿って仮想トークンを登録できます。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Register Smart Card or Token]**（スマート カードまたはトークンの登録）をクリックします。 [Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

USB eToken の登録

1. USB eToken ドライバがインストールされていることを確認します。

   注記： 詳しくは、USB eToken の取扱説明書を参照してください。
2. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
3. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
4. 右側のパネルで、**[Register Smart Card or Token]**（スマート カードまたはトークンの登録）をクリックします。 [Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。
5. 画面に表示される説明に沿って操作します。

その他の証明情報の登録

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。

3. 右側のパネルで、**[Register Credentials]**（証明情報の登録）をクリックします。 [Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。

4. 画面に表示される説明に沿って操作します。

一般的なタスク

Credential Manager の[My Identity]（個人 ID）ページには、すべてのユーザがアクセスできます。 [My Identity]ページから、次のことができます。

- 仮想トークンの作成
- Windows ログオン パスワードの変更
- トークン PIN の管理
- ID の管理
- コンピュータのロック

注記： このオプションは、Credential Manager のクラシック ログオン画面が有効に設定されている場合にのみ利用できます。 29 ページの 「例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法」を参照してください。

仮想トークンの作成

仮想トークンの機能は、Java Card や USB eToken とよく似ています。 このトークンは、コンピュータのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。 仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

新しい仮想トークンを作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Virtual Token]**（仮想トークン）をクリックします。 [Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。

注記： **[Virtual Token]**（仮想トークン）オプションがない場合は、16 ページの 「その他の証明情報の登録」の手順を実行します。

4. 画面に表示される説明に沿って操作します。

Windows ログオン パスワードの変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Change Windows Password]**（Windows パスワードの変更）をクリックします。
4. **[Old password]**（古いパスワード）ボックスに、古いパスワードを入力します。
5. **[New Password]**（新しいパスワード）ボックスおよび**[Confirm password]**（パスワードの確認）ボックスに新しいパスワードを入力します。
6. **[Finish]**（完了）をクリックします。

トークン PIN の変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Change Token PIN]**（トークン PIN の変更）をクリックします。
4. PIN を変更するトークンを選択して**[Next]**（次へ）をクリックします。
5. 画面の説明に沿って操作し、PIN の変更を完了します。

ID の管理

システムからの ID の消去

注記： この操作は、Windows ユーザ アカウントには影響しません。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Clear Identity for this Account]**（このアカウントの ID の消去）をクリックします。
4. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。 ID がログオフされ、システムから削除されます。

コンピュータのロック

この機能は、Credential Manager を使用して Windows にログオンした場合に利用できます。 席を離れている間のコンピュータの安全を確保するには、作業環境のロック機能を使用します。 これにより、不正なユーザによるコンピュータへのアクセスを防ぐことができます。 このロックは、自分自身と、コンピュータ上の管理者グループのメンバのみが解除できます。

注記： このオプションは、Credential Manager のクラシック ログオン画面が有効に設定されている場合にのみ利用できます。29 ページの 「例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法」を参照してください。

コンピュータのロック解除に Java Card、指紋認証システム、またはトークンが必要となるように作業環境のロック機能を設定することで、セキュリティを強化できます。 詳しくは、29 ページの 「Credential Manager の設定」を参照してください。

コンピュータをロックするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Lock Workstation]**（作業環境をロック）をクリックします。 Windows のログオン画面が表示されます。 コンピュータのロックを解除するには、Windows パスワードまたは[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）を使用する必要があります。

Windows のログオンの使用

ローカル コンピュータまたはネットワーク ドメインのどちらでも、Credential Manager を使用して Windows にログオンできます。 初めて Credential Manager にログオンすると、ローカルの Windows ユーザ アカウントが Windows ログオン サービス用のアカウントとして自動的に追加されます。

Credential Manager を使用した Windows へのログオン

Credential Manager を使用して、Windows のネットワークまたはローカル アカウントにログオンできます。

1. Windows へのログオン用に指紋を登録してある場合は、指を押し当ててログオンします。
2. Windows へのログオン用に指紋を登録していない場合は、画面の左上隅にある指紋アイコンの隣のキーボード アイコンをクリックします。 [Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）が起動します。
3. **[User name]**（ユーザ名）の矢印→自分の名前の順にクリックします。
4. **[Password]**（パスワード）ボックスにパスワードを入力して**[Next]**（次へ）をクリックします。

5. **[More]**（詳細）→**[Wizard Options]**（ウィザード オプション）の順に選択します。
   a. 次回コンピュータにログオンした時にこの名前を初期設定のユーザ名にする場合は、**[Use last user name on next logon]**（前回のユーザ名を次のログオン時に使用）チェック ボックスにチェックを入れます。
   b. このログオン ポリシーを初期設定の認証方法にする場合は、**[Use last policy on next logon]**（前回のポリシーを次のログオン時に使用）チェック ボックスにチェックを入れます。
6. 画面に表示される説明に沿って操作します。 認証情報が正しい場合は、Windows アカウントおよび Credential Manager にログオンします。

アカウントの追加

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルで、**[Windows Logon]**（Windows のログオン）→**[Add a Network Account]**（ネットワーク アカウントの追加）の順にクリックします。 [Add Network Account Wizard]（ネットワーク アカウントの追加ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

アカウントの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルで、**[Windows Logon]**（Windows のログオン）→**[Manage Network Accounts]**（ネットワーク アカウントの管理）の順にクリックします。 **[Manage Network Accounts]**ダイアログ ボックスが表示されます。
4. 削除するアカウントをクリックして**[Remove]**（削除）をクリックします。
5. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。
6. **[OK]**をクリックします。

シングルサインオンの使用

Credential Manager には、複数のインターネットおよび Windows プログラム用のユーザ名とパスワードを格納し、ユーザが登録されたプログラムにアクセスすると自動的にログオン証明情報を入力する、シングルサインオン機能があります。

注記： シングルサインオンの重要な機能は、セキュリティとプライバシです。 証明情報はすべて暗号化されており、Credential Manager へのログオンに成功した後にだけ使用できます。

注記： セキュリティ保護されたサイトまたはプログラムにログオンする前に、Java Card、指紋認証システム、またはトークンを使用して認証証明情報を検証するように、シングルサインオンを設定することもできます。 この機能は、銀行口座番号などの個人情報が含まれているプログラムまたは Web サイトにログオンする場合に特に有効です。 詳しくは、29 ページの 「Credential Manager の設定」を参照してください。

新しいアプリケーションの登録

Credential Manager では、Credential Manager にログオンしている間に起動するアプリケーションをすべて登録するよう要求されます。 アプリケーションを手動で登録することもできます。

自動登録の使用

1. ログオンが必要なアプリケーションを起動します。
2. プログラムまたは Web サイトのパスワード ダイアログ ボックスで[Credential Manager SSO]（証明情報マネージャ シングルサインオン）アイコンをクリックします。
3. プログラムまたは Web サイトのパスワードを入力して**[OK]**をクリックします。 **[Credential Manager Single Sign On]**（証明情報マネージャ シングルサインオン）ダイアログ ボックスが開きます。
4. **[More]**（詳細）をクリックして以下のオプションのどれかを選択します。
   - [Do not use SSO for this site or application.]（このサイトまたはアプリケーションではシングルサインオン（SSO）を使用しない。）
   - [Prompt to select account for this application.]（このアプリケーションのアカウントの選択画面を表示する。）
   - [Fill in credentials but do not submit.]（証明情報を入力するが送信はしない。）
   - [Authenticate user before submitting credentials.]（証明情報を送信する前にユーザ認証を行う。）
   - [Show SSO shortcut for this application.]（このアプリケーションの SSO ショートカットを表示する。）
5. **[Yes]**（はい）をクリックして、登録を完了します。

手動（ドラッグ アンド ドロップ）登録の使用

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルで、**[Single Sign On]**（シングルサインオン）→**[Register New Application]**（新しいアプリケーションの追加）の順にクリックします。 [SSO Application Wizard]（SSO アプリケーション ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

アプリケーションおよび証明情報の管理

アプリケーション プロパティの変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。
4. 変更するアプリケーション エントリをクリックして**[Properties]**.（プロパティ）をクリックします。
5. **[General]**（全般）タブをクリックして、アプリケーション名および説明を変更します。 該当する設定の横にあるチェック ボックスにチェックを入れるか外して、設定を変更します。
6. **[Script]**（スクリプト）タブをクリックして、SSO アプリケーション スクリプトを表示し、編集します。
7. **[OK]**をクリックします。

シングルサインオンからのアプリケーションの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。
4. 削除するアプリケーション エントリをクリックして**[Remove]**（削除）をクリックします。
5. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。
6. **[OK]**をクリックします。

アプリケーションのエクスポート

アプリケーションをエクスポートして、シングルサインオン アプリケーション スクリプトのバックアップ コピーを作成できます。 このファイルは、後でシングルサインオン データの復元に使用できます。 これは、証明情報だけが含まれている ID バックアップ ファイルを補うものとして機能します。

アプリケーションをエクスポートするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。

4. エクスポートするアプリケーション エントリをクリックします。**[More]**（詳細）→**[Applications]**（アプリケーション）→**[Export Script]**（スクリプトのエクスポート）の順にクリックします。

5. 画面の説明に沿って操作し、エクスポートを完了します。

6. **[OK]**をクリックします。

アプリケーションのインポート

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。

4. インポートするアプリケーション エントリをクリックします。**[More]**（詳細）→**[Applications]**（アプリケーション）→**[Import Script]**（スクリプトのインポート）の順に選択します。

5. 画面の説明に沿って操作し、インポートを完了します。

6. **[OK]**をクリックします。

証明情報の変更

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。

4. 変更するアプリケーション エントリをクリックして**[More]**（詳細）をクリックします。

5. 以下のオプションのどれかを選択します。

   - Applications（アプリケーション）
     - Add New（新規追加）
     - Remove（削除）
     - Properties（プロパティ）
     - Import Script（スクリプトのインポート）
     - Export Script（スクリプトのエクスポート）
   - 証明情報
     - Create New（新規作成）
   - View Password（パスワードの表示）

注記： パスワードを表示するには、事前に ID の認証を行う必要があります。

6. 画面に表示される説明に沿って操作します。

7. **[OK]**をクリックします。

アプリケーションの保護機能の使用

この機能を使用して、アプリケーションへのアクセス設定を行えます。 以下の基準に基づいてアクセスを制限できます。

- ユーザのカテゴリ
- 使用する時間
- 無操作の状態

アプリケーションへのアクセス制限

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。 **[Application Protection Service]**（アプリケーション保護サービス）ダイアログ ボックスが表示されます。

4. アクセスを管理したいユーザのカテゴリを選択します。

注記：　カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）を選択する必要がある場合があります。

5. **[Add]**（追加）をクリックします。 [Add a Program Wizard]（プログラムの追加ウィザード）が起動します。

6. 画面に表示される説明に沿って操作します。

アプリケーションの保護の解除

アプリケーションのアクセス制限を解除するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。 **[Application Protection Service]**（アプリケーション保護サービス）ダイアログ ボックスが表示されます。

4. アクセスを管理したいユーザのカテゴリを選択します。

注記：　カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）をクリックする必要がある場合があります。

5. 削除するアプリケーション エントリをクリックして**[Remove]**（削除）をクリックします。

6. **[OK]**をクリックします。

保護されたアプリケーションの制限設定の変更

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。 **[Application Protection Service]**（アプリケーション保護サービス）ダイアログ ボックスが表示されます。

4. アクセスを管理したいユーザのカテゴリを選択します。

注記： カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）をクリックする必要がある場合があります。

5. 変更するアプリケーションをクリックして**[Properties]**（プロパティ）をクリックします。 そのアプリケーションの**[Properties]**（プロパティ）ダイアログ ボックスが開きます。

6. **[General]**（全般）タブをクリックします。 以下の設定のどれかを選択します。

   - [Disabled (Cannot be used)]（無効（使用不可））
   - [Enabled (Can be used without restrictions)]（有効（無制限に使用可能））
   - [Restricted (Usage depends on settings)]（制限あり（使用制限は設定により異なる））

7. [Restricted]（制限あり）を選択した場合、以下の設定が利用可能になります。

   a. 時間、曜日、または日付に基づいて使用を制限する場合は、**[Schedule]**（スケジュール）タブをクリックして設定を行います。

   b. 無操作状態に基づいて使用を制限する場合は、**[Advanced]**（詳細）タブをクリックして無操作の期間を選択します。

8. **[OK]**をクリックして、アプリケーションの**[Properties]**（プロパティ）ダイアログ ボックスを閉じます。

9. **[OK]**をクリックします。

高度なタスク（管理者のみ）

Credential Manager の[Authentication and Credentials]（認証および証明情報）ページおよび[Advanced Settings]（詳細設定）ページは、管理者権限を持つユーザだけが使用できます。 これらのページから、次のタスクを実行できます。

- ユーザおよび管理者のログオン方法の指定
- カスタム認証要件の設定
- 証明情報のプロパティの設定
- Credential Manager の設定

ユーザおよび管理者のログオン方法の指定

[Authentication and Credentials]（認証および証明情報）ページで、ユーザまたは管理者のどちらかに、どのような種類または組み合わせの証明情報が必要かを指定できます。

ユーザまたは管理者のログオン方法を指定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Authentication and Credentials]**（認証および証明情報）の順にクリックします。
3. 右側のパネルで、**[Authentication]**（認証）タブをクリックします。
4. カテゴリの一覧から、カテゴリ（**[Users]**（ユーザ）または**[Administrators]**（管理者））をクリックします。
5. 一覧から、認証方法の種類または組み合わせをクリックします。
6. **[Apply]**（適用）→**[OK]**の順にクリックします。

カスタム認証要件の設定

[Authentication and Credentials]（認証および証明情報）ページの[Authentication]（認証）タブに、必要な認証証明情報のセットが一覧表示されない場合は、カスタム要件を作成できます。

カスタム要件を設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Authentication and Credentials]**（認証および証明情報）の順にクリックします。
3. 右側のパネルで、**[Authentication]**（認証）タブをクリックします。
4. カテゴリの一覧から、カテゴリ（**[Users]**（ユーザ）または**[Administrators]**（管理者））をクリックします。
5. 認証方法の一覧から、**[Custom]**（カスタム）をクリックします。
6. **[Configure]**（設定）をクリックします。
7. 使用する認証方法を選択します。
8. 以下のどちらかの項目をクリックして、方法の組み合わせを選択します。
   - AND を使用して認証方法を組み合わせる

     （ユーザはログオンするたびに、チェックを入れたすべての方法で認証する必要があります）
   - OR を使用して複数の認証方法のうち 1 つを要求する

     （ユーザはログオンするたびに、チェックを入れた方法のどれかを選択できます）
9. **[OK]**をクリックします。
10. **[Apply]**（適用）→**[OK]**の順にクリックします。

証明情報のプロパティの設定

[Authentication and Credentials]（認証および証明情報）ページの[Credentials]（証明情報）タブで、使用可能な認証方法の一覧を表示して設定を変更できます。

証明情報を設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Authentication and Credentials]**（認証および証明情報）の順にクリックします。
3. 右側のパネルで、**[Credentials]**（証明情報）タブをクリックします。

4. 変更する証明情報の種類をクリックします。 次のどれかの方法で証明情報を変更できます。
   - 証明情報を登録するには、**[Register]**（登録）をクリックし、画面の説明に沿って操作します。
   - 証明情報を削除するには、**[Clear]**（クリア）をクリックし、確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。
   - 証明情報のプロパティを変更するには、**[Properties]**（プロパティ）をクリックし、画面の説明に沿って操作します。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。

Credential Manager の設定

[Settings]（設定）ページから、以下のタブを使用して各種の設定にアクセスし、変更することができます。

- General（全般）：基本的な設定を変更できます。
- Single Sign On（シングルサインオン）：現在のユーザに対するシングルサインオンの動作方法の設定（たとえば、ログオン画面の検出、登録されたログオン ダイアログへの自動ログオン、パスワードの表示などの処理方法）を変更できます。
- Services and Applications（サービスおよびアプリケーション）：使用可能なサービスを表示して、それらのサービスの設定を変更できます。
- Security（セキュリティ）：指紋認証ソフトウェアを選択して、指紋認証システムのセキュリティ レベルを調整できます。
- Smart Cards and Tokens（スマート カードおよびトークン）：使用可能なすべての Java Card およびトークンのプロパティを表示して変更できます。

Credential Manager の設定を変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、変更する設定が含まれるタブをクリックします。
4. 画面の説明に沿って操作し、設定を変更します。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。

例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、**[General]**（全般）タブをクリックします。

4. **[Select the way users log on to Windows (requires restart)]**（ユーザが Windows へログオンする方法の選択（再起動が必要））で、**[Use Credential Manager with classic logon prompt]**（証明情報マネージャでクラシック ログオン画面を使用する）チェック ボックスにチェックを入れます。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。
6. コンピュータを再起動します。

注記： **[Use Credential Manager with classic logon prompt]**（証明情報マネージャでクラシック ログオン画面を使用する）チェック ボックスにチェックを入れると、コンピュータをロックできるようになります。20 ページの 「コンピュータのロック」を参照してください。

例 2：[Advanced Settings]（詳細設定）ページを使用して、シングルサインオンの前にユーザ確認を要求する方法

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、**[Single Sign On]**（シングルサインオン）タブをクリックします。
4. **[When registered logon dialog or Web page is visited]**（登録したログオン ダイアログまたは Web ページが表示された時の動作）で、**[Authenticate user before submitting credentials]**（証明情報を送信する前にユーザの認証を行う）チェック ボックスにチェックを入れます。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。
6. コンピュータを再起動します。

3　Embedded Security for HP ProtectTools

注記：　Embedded Security for HP ProtectTools を使用するには、統合された TPM（Trusted Platform Module）セキュリティ チップがコンピュータに内蔵されている必要があります。

Embedded Security for HP ProtectTools は、ユーザ データや証明情報を不正なアクセスから保護します。 このソフトウェア モジュールには、以下のセキュリティ機能があります。

- 高度な Microsoft® EFS（Encryption File System）ファイルおよびフォルダの暗号化
- ユーザ データを保護するための PSD（Personal Secure Drive）の作成
- データ管理機能（キー階層のバックアップや復元など）
- Embedded Security ソフトウェアの使用時にデジタル証明情報の操作を保護するための他社製のアプリケーション（Microsoft Outlook や Internet Explorer など）のサポート

TPM 内蔵セキュリティ チップを使用すると、HP ProtectTools セキュリティマネージャの他のセキュリティ機能を強化したり有効にしたりできます。 たとえば、Credential Manager for HP ProtectTools では、内蔵チップを Windows へのログオン時の認証要素として使用できます。 一部のモデルでは、TPM 内蔵セキュリティ チップを使用して、BIOS Configuration for HP ProtectTools からアクセスする高度な BIOS セキュリティ機能を有効にすることもできます。

セットアップ手順

注意： セキュリティ上の危険にさらされないようにするために、IT 管理者が内蔵セキュリティ チップを直ちに初期化することを強くおすすめします。 内蔵セキュリティ チップを初期化しない場合、不正なユーザ、コンピュータ ワーム、またはウィルスがコンピュータのオーナシップを奪い、緊急リカバリ アーカイブの処理やユーザ アクセスの設定など所有者のタスクを制御してしまう可能性があります。

以下の 2 つの項目の手順に沿って操作し、内蔵セキュリティ チップを有効にして初期化します。

内蔵セキュリティ チップの有効化

内蔵セキュリティ チップは、[Computer Setup]ユーティリティで有効にする必要があります。 この手順は、BIOS Configuration for HP ProtectTools では実行できません。

内蔵セキュリティ チップを有効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に[F10 = ROM Based Setup]（ROM ベースのセットアップ）というメッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 管理者パスワードを設定していない場合は、矢印キーを使用して**[Security]**（セキュリティ設定）→**[Setup password]**（セットアップ パスワード）の順に選択して enter キーを押します。
3. **[New password]**（新しいパスワード）および**[Verify new password]**（新しいパスワードの確認）ボックスにパスワードを入力して f10 キーを押します。
4. **[Security]**（セキュリティ設定）メニューで、矢印キーを使用して**[TPM Embedded Security]**（TPM 内蔵セキュリティ）を選択し、enter キーを押します。
5. **[Embedded Security]**（内蔵セキュリティ）にデバイスが表示されない場合、**[Available]**（利用可能）を選択します。
6. **[Embedded security device state]**（内蔵セキュリティ デバイスの状態）を選択し、**[Enable]**（有効にする）に変更します。
7. f10 キーを押して、Embedded Security の設定への変更を確定します。
8. 設定を保存して[Computer Setup]を終了するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（設定を保存して終了）の順に選択します。 次に、画面の説明に沿って操作します。

内蔵セキュリティ チップの初期化

内蔵セキュリティの初期化プロセスでは、以下のことを行います。

- 内蔵セキュリティ チップの所有者のパスワードを設定します。これにより、内蔵セキュリティ チップ上のすべての所有者機能へのアクセスが保護されます。
- 緊急リカバリ アーカイブをセットアップします。緊急リカバリ アーカイブとは、すべてのユーザの基本ユーザ キーを再暗号化できるようにするための保護された記憶領域です。

内蔵セキュリティ チップを初期化するには、以下の手順で操作します。

1. タスク バーの右端の通知領域にある[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコンを右クリックして、**[Embedded Security Initialization]**（内蔵セキュリティの初期化）を選択します。

   [HP ProtectTools Embedded Security Initialization Wizard]（HP ProtectTools Embedded Security 初期化ウィザード）が起動します。

2. 画面に表示される説明に沿って操作します。

基本ユーザ アカウントのセットアップ

Embedded Security で基本ユーザ アカウントをセットアップすると、次のタスクが実行されます。

- 暗号化された情報を保護するための基本ユーザ キーが生成され、その基本ユーザ キーを保護するための基本ユーザ キーのパスワードが設定されます。
- 暗号化されたファイルおよびフォルダを格納するための PSD（Personal Secure Drive）が設定されます。

注意： 基本ユーザ キーのパスワードは保護しておいてください。 このパスワードがないと、暗号化されたデータにアクセスしたり復元したりできなくなります。

基本ユーザ アカウントをセットアップしてユーザ セキュリティ機能を有効にするには、以下の手順で操作します。

1. [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動していない場合は、**[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザーの設定）の順にクリックします。
3. 右側のパネルで、**[Embedded Security Features]**（内蔵セキュリティの機能）の**[Configure]**（設定）をクリックします。

   [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

   注記： セキュリティ保護された電子メールを使用するには、最初に、Embedded Security で作成されたデジタル証明情報を使用するように電子メール クライアントを設定する必要があります。 デジタル証明情報が使用できない場合は、証明機関から取得する必要があります。 電子メールを設定してデジタル証明情報を取得する手順については、電子メール クライアントのヘルプを参照してください。

一般的なタスク

基本ユーザ アカウントのセットアップを完了すると、以下のタスクを実行できます。

- ファイルおよびフォルダの暗号化
- 暗号化された電子メールの送受信

Personal Secure Drive（PSD）の使用

PSD のセットアップを完了すると、次回のログオンで、基本ユーザ キーのパスワードを入力するよう要求されます。 基本ユーザ キーのパスワードを正しく入力すると、Windows エクスプローラから直接 PSD にアクセスできます。

ファイルおよびフォルダの暗号化

暗号化ファイルを操作する場合は、以下の規則を考慮してください。

- 暗号化できるファイルおよびフォルダは、NTFS パーティション上のものだけです。 FAT パーティション上のファイルおよびフォルダは暗号化できません。
- システム ファイルや圧縮されたファイルは暗号化できません。また、暗号化されたファイルは圧縮できません。
- 一時フォルダは、ハッカーの関心を引く可能性があるため、暗号化するようにしてください。
- ファイルまたはフォルダを初めて暗号化した時、回復ポリシーが自動的にセットアップされます。 暗号化証明情報や秘密キーをなくした場合でも、このポリシーによって、回復エージェントを使用して情報の暗号化を解除できるようになります。

ファイルおよびフォルダを暗号化するには、以下の手順で操作します。

1. 暗号化するファイルまたはフォルダを右クリックします。
2. **[Encrypt]**（暗号化）をクリックします。
3. 以下のオプションのどちらかをクリックします。
   - **[Apply changes to this folder only]**（このフォルダにのみ変更を適用する）
   - **[Apply changes to this folder, subfolders, and files]**（このフォルダ、およびサブフォルダとファイルに変更を適用する）
4. **[OK]**をクリックします。

暗号化された電子メールの送受信

Embedded Security では、暗号化された電子メールの送受信を行うことができますが、その手順は電子メールのアクセスに使用しているプログラムによって異なります。 詳しくは、Embedded Security のヘルプおよび使用している電子メール アプリケーションのヘルプを参照してください。

基本ユーザ キーのパスワードの変更

基本ユーザ キーのパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザーの設定）の順にクリックします。
3. 右側のパネルで、**[Basic User Key password]**（基本ユーザ キーのパスワード）の**[Change]**（変更）をクリックします。
4. 古いパスワードを入力した後、新しいパスワードを設定して確定します。
5. **[OK]**をクリックします。

高度なタスク

バックアップおよび復元

Embedded Security のバックアップ機能では、緊急の場合に復元される証明情報を含むアーカイブが作成されます。

バックアップ ファイルの作成

バックアップ ファイルを作成するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側のパネルで、**[Backup]**をクリックします。 HP Embedded Security for ProtectTools Backup Wizard（HP Embedded Security for ProtectTools バックアップ ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

バックアップ ファイルからの証明データの復元

バックアップ ファイルからデータを復元するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側のパネルで、**[Restore]**（復元）をクリックします。 HP Embedded Security for ProtectTools Backup Wizard（HP Embedded Security for ProtectTools バックアップ ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

所有者のパスワードの変更

所有者のパスワードを変更するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Owner Password]**（所有者のパスワード）の**[Change]**（変更）をクリックします。
4. 古い所有者のパスワードを入力した後、新しい所有者のパスワードを設定して確定します。
5. **[OK]**をクリックします。

ユーザ パスワードの再設定

ユーザが忘れたパスワードを管理者に再設定してもらうことができます。 詳しくは、ヘルプを参照してください。

Embedded Security の有効化および無効化

セキュリティ機能を使用しないで操作する場合は、Embedded Security の機能を無効にすることができます。

Embedded Security の機能は、次の 2 種類のレベルで有効または無効にすることができます。

- 一時的な無効化：このオプションを使用すると、Windows の再起動時に Embedded Security が自動的に再び有効になります。 このオプションは、初期設定ですべてのユーザが使用できます。
- 永続的な無効化：このオプションを使用すると、Embedded Security を再び有効にするには所有者のパスワードが必要になります。 このオプションは、管理者だけが使用できます。

Embedded Security の永続的な無効化

Embedded Security を永続的に無効にするには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Embedded Security]**の**[Disable]**（無効にする）をクリックします。
4. 入力画面で所有者のパスワードを入力して**[OK]**をクリックします。

Embedded Security の永続的な無効化の後の有効化

Embedded Security を永続的に無効にした後で再び有効にするには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。

3. 右側のパネルで、**[Embedded Security]**の**[Enable]**（有効にする）をクリックします。

4. 入力画面で所有者のパスワードを入力して**[OK]**をクリックします。

移行ウィザードによるキーの移行

移行は、キーや証明情報の管理、復元、転送などを行うことができる、高度な管理者タスクです。

移行について詳しくは、Embedded Security のヘルプを参照してください。

4 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools は、オプションのカード リーダーが装備されたコンピュータでの Java Card のセットアップおよび設定を管理します。

Java Card Security を使用すると、次のタスクを実行できます。

- Java Card のセキュリティ機能にアクセスできます。
- [Computer Setup]ユーティリティを使用して、電源投入時の環境で Java Card の認証を有効にすることができます。
- Java Card を管理者およびユーザに個別に設定できます。 オペレーティング システムがロードされる前に、ユーザは Java Card を挿入し、PIN を入力する必要があります。
- Java Card のユーザ認証を行うための PIN の設定および変更を行えます。

一般的なタスク

[General]（全般）ページを使用すると、次のタスクを実行できます。

- Java Card の PIN の変更
- カード リーダーの選択

注記： カード リーダーでは、Java Card とスマート カードの両方を使用します。 この機能は、コンピュータに複数のカード リーダーが装備されている場合に使用できます。

Java Card の PIN の変更

Java Card の PIN を変更するには、以下の手順で操作します。

注記： Java Card の PIN は、4 ～ 8 桁の半角数字にする必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[General]**（全般）をクリックします。
3. PIN が設定されている Java Card をカード リーダーに挿入します。
4. 右側のパネルで、**[Change]**（変更）をクリックします。
5. **[Change PIN]**（PIN の変更）ダイアログ ボックスで、**[Current PIN]**（現在の PIN）ボックスに現在の PIN を入力します。
6. **[New PIN]**（新しい PIN）ボックスに新しい PIN を入力し、**[Confirm New PIN]**（新しい PIN の確認入力）ボックスに PIN を再度入力します。
7. **[OK]**をクリックします。

カード リーダーの選択

Java Card を使用する前に、Java Card Security for ProtectTools で正しいカード リーダーが選択されていることを確認してください。 正しいリーダーが選択されていないと、一部の機能が使用できなくなるか、正しく表示されない場合があります。 さらに、カード リーダー ドライバが正しくインストールされ、Windows の[デバイス マネージャ]に正しく表示される必要があります。

カード リーダーを選択するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[General]**（全般）をクリックします。
3. Java Card をカード リーダーに挿入します。
4. 右側のパネルの**[Selected card reader]**（スマート カード リーダー）で正しいリーダーをクリックします。

高度なタスク（管理者のみ）

[Advanced]（アドバンス）ページを使用すると、次のタスクを実行できます。

- Java Card の PIN の割り当て
- Java Card への名前の割り当て
- 電源投入時認証の設定
- Java Card のバックアップおよびリストア（復元）

注記： **[Advanced]**（アドバンス）ページを表示するには、Windows 管理者権限を持っている必要があります。

Java Card の PIN の割り当て

Java Card Security for ProtectTools で Java Card を使用できるようにするには、Java Card に名前と PIN を割り当てる必要があります。

Java Card に PIN を割り当てるには、以下の手順で操作します。

注記： Java Card の PIN は、4 ～ 8 桁の半角数字にする必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. 新しい Java Card をカード リーダーに挿入します。
4. **[New Card]**（新しいカード）ダイアログ ボックスが表示されたら、**[New display name]**（新しい表示名）ボックスに新しい名前を、**[New PIN]**（新しい PIN）ボックスに新しい PIN を入力し、**[Confirm New PIN]**（新しい PIN の確認入力）ボックスに PIN を再度入力します。
5. **[OK]**をクリックします。

Java Card への名前の割り当て

電源投入時認証に Java Card を使用できるようにするには、Java Card に名前を割り当てる必要があります。

Java Card に名前を割り当てるには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. Java Card をカード リーダーに挿入します。

注記：　このカードにまだ PIN を割り当てていない場合は、**[New Card]**（新しいカード）ダイアログ ボックスが表示され、ここで新しい名前および PIN を入力できます。

4. 右側のパネルで、**[Display name]**（表示名）の**[Change]**（変更）をクリックします。
5. **[Name]**（名前）ボックスに、Java Card の名前を入力します。
6. **[PIN]**ボックスに、現在の Java Card の PIN を入力します。
7. **[OK]**をクリックします。

電源投入時認証の設定

電源投入時認証が有効になると、Java Card を使用してコンピュータを起動することが必要になります。

Java Card の電源投入時認証を有効にするプロセスには、以下の手順が含まれます。

1. BIOS Configuration または[Computer Setup]ユーティリティで、Java Card の電源投入時認証サポートを有効にします。 詳しくは、53 ページの 「スマート カードの電源投入時認証サポートの有効/無効の設定」を参照してください。
2. Java Card Security for ProtectTools で、Java Card の電源投入時認証を有効にします。
3. 管理者 Java Card を作成し、有効にします。

Java Card の電源投入時認証の有効化および管理者 Java Card の作成

Java Card の電源投入時認証を有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. Java Card をカード リーダーに挿入します。

注記： このカードにまだ名前および PIN を割り当てていない場合は、**[New Card]**（新しいカード）ダイアログ ボックスが表示され、ここで新しい名前および PIN を入力できます。

4. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[Enable]**（有効にする）チェック ボックスにチェックを入れます。
5. **[Computer Setup Password]**（[Computer Setup]のパスワード）ダイアログ ボックスで、[Computer Setup]ユーティリティのパスワードを入力して**[OK]**をクリックします。
6. DriveLock をまだ有効にしていない場合は、Java Card の PIN を入力して**[OK]**をクリックします。

   または

   DriveLock をすでに有効にしている場合は、以下の手順で操作します。

   a. **[Make Java card identity unique]**（Java Card の ID を固有のものにする）をクリックします。

      または

      [Make the Java card identity the same as the DriveLock password]（Java Card の ID を DriveLock パスワードと同じにする）をクリックします。

      注記： コンピュータで DriveLock が有効になっていると、Java Card の ID を DriveLock の user password（ユーザ パスワード）と同じものに設定できます。これにより、コンピュータを起動するときに、Java Card のみを使用して DriveLock と Java Card の両方を認証できるようになります。

   b. 必要に応じて、**[DriveLock password]**（DriveLock パスワード）ボックスに DriveLock の user password（ユーザ パスワード）を入力し、**[Confirm password]**（パスワードの確認）ボックスにパスワードを再度入力します。

   c. Java Card の PIN を入力します。

   d. **[OK]**をクリックします。

7. リカバリ ファイルを作成するよう要求されたら、**[Cancel]**（キャンセル）をクリックして後でリカバリ ファイルを作成するか、または**[OK]**をクリックし、[HP ProtectTools Backup Wizard]（HP ProtectTools バックアップ ウィザード）の画面の説明に沿って操作し、ここでリカバリ ファイルを作成します。

注記： 詳しくは、9 ページの 「HP ProtectTools Backup and Restore」を参照してください。

ユーザ Java Card の作成

注記：　ユーザ Java Card を作成するには、電源投入時認証および管理者カードが設定されている必要があります。

ユーザ Java Card を作成するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. ユーザ カードとして使用する Java Card を挿入します。
4. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[User card identity]**（ユーザ用カードの ID）の横にある**[Create]**（作成）をクリックします。
5. ユーザ Java Card の PIN を入力して**[OK]**をクリックします。

Java Card の電源投入時認証の無効化

Java Card の電源投入時認証を無効にすると、コンピュータにアクセスするために Java Card を使用する必要はなくなります。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. 管理者 Java Card を挿入します。
4. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[Enable]**（有効にする）チェック ボックスのチェックを外します。
5. Java Card の PIN を入力して**[OK]**をクリックします。

5 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools を使用すると、[Computer Setup]ユーティリティのセキュリティ設定にアクセスできます。 これにより、[Computer Setup]で管理されるシステムのセキュリティ機能に Windows から簡単にアクセスできるようになります。

BIOS Configuration を使用すると、次のことを行えます。

- 電源投入時パスワードおよび管理者パスワードを管理できます。
- 内蔵セキュリティ認証サポートの有効化など、電源投入時のその他の認証機能を設定できます。
- CD-ROM のブートや各種ハードウェア ポートなど、ハードウェア機能を有効および無効に設定できます。
- マルチブートの有効化および起動順序の変更を含む、ブート オプションを設定できます。

注記： BIOS Configuration for HP ProtectTools にある機能の多くは、[Computer Setup]でも使用できます。

一般的なタスク

BIOS Configuration を使用すると、通常は起動時に f10 キーを押して[Computer Setup]を使用することでしかアクセスできない、各種のコンピュータ設定を管理できます。

ブート オプションの管理

BIOS Configuration を使用すると、コンピュータの起動や再起動に実行されるタスクに対する各種の設定を管理できます。

ブート オプションを管理するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。

注記： BIOS の管理者パスワードの入力画面は、[Computer Setup]のパスワードがすでに設定されている場合にのみ表示されます。 [Computer Setup]のパスワードの設定について詳しくは、56 ページの 「セットアップ パスワードの設定」を参照してください。

4. 左側のパネルで、**[System Configuration]**（システム コンフィギュレーション）をクリックします。
5. 右側のパネルで、f9、f10、および f12 と、**[Express Boot Popup Delay（Sec）]**（高速ブート ポップアップ遅延（秒））に対する遅延時間（秒単位）を選択します。
6. **[MultiBoot]**（マルチブート）を有効または無効にします。
7. マルチブートを有効にしている場合は、ブート デバイスを選択し、上向きの矢印または下向きの矢印をクリックして一覧内の順序を調整することで、起動順序を選択します。
8. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

システム コンフィギュレーション オプションの有効/無効の設定

注記： 次の項目の一部は、お使いのコンピュータでサポートされていない場合があります。

デバイスまたはセキュリティ オプションの有効/無効を切り替えるには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]** をクリックします。
4. 左側のパネルで**[System Configuration]**（システム コンフィギュレーション）をクリックしてから、システム コンフィギュレーション オプションの有効/無効を切り替えるか、右側のパネルで次のどれかのシステム コンフィギュレーション オプションの設定を行います。
   - Port Options（ポート オプション）
     - Serial Port（シリアル ポート）
     - Infrared Port（赤外線ポート）
     - Parallel Port（パラレル ポート）
     - SD Slot（SD スロット）
     - USB Port（USB ポート）
     - 1394 Port（1394 ポート）
     - Cardbus Slot（CardBus スロット）
     - ExpressCard slot（ExpressCard スロット）
   - Boot Options（ブート オプション）
     - f9, f10, and f12 Delay (Sec)（f9、f10、および f12 の遅延（秒））
     - MultiBoot（マルチブート）
     - Express Boot Popup Delay (Sec)（高速ブート ポップアップ遅延（秒））
     - CD-ROM Boot（CD-ROM ドライブからのブート）
     - Floppy Boot（フロッピーディスク ドライブからのブート）
     - Internal Network Adapter Boot（内蔵ネットワーク アダプタ ブート）
     - Internal Network Adapter Boot Mode (PXE or RPL)（内蔵ネットワーク アダプタ ブート モード（PXE または RPL））
     - Boot Order（ブート順序）
   - Device Configurations（デバイス設定）
     - NumLock at Boot（ブート時 NumLock）
     - Swapping fn/ctrl Keys（[fn]/[ctrl]キーの切り替え）

- Multiple Pointing Devices（マルチポインティング デバイス）
- USB Legacy Support（USB レガシー サポート）
- Parallel port mode (standard, bidirectional, EPP, or ECP)（パラレル ポート モード：EPP（Enhanced Parallel Port）、標準、双方向、または ECP（Enhanced Capabilities Port））
- Data Execution Prevention（データ実行防止）
- SATA Native Mode（SATA ネイティブ モード）
- Dual Core CPU（デュアル コア CPU）
- Automatic Intel® SpeedStep Functionality Support（Automatic Intel SpeedStep 機能サポート）
- Fan Always on While on AC Power（外部電源の使用中は常にファンをオンにする）
- BIOS DMA Data Transfers（BIOS ATA DMA 転送）
- Intel or AMD PSAE Execution Disable（Intel または AMD PSAE の実行無効設定）

- Built-In Device Options（内蔵デバイス オプション）
  - Embedded WLAN Device Radio（内蔵無線 LAN デバイスの無線）
  - Embedded WWAN Device Radio（内蔵無線 WAN デバイスの無線）
  - Embedded Bluetooth® Device Radio（内蔵 Bluetooth デバイスの無線）
  - LAN/WLAN Switching（LAN/無線 LAN の切り替え）
  - Wake on LAN from Off（電源オフ状態からの Wake on LAN の実行）

5. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックして変更を保存してから終了します。

高度なタスク

HP ProtectTools アドオン モジュールの設定の管理

HP ProtectTools セキュリティ マネージャの一部の機能は、BIOS Configuration で管理できます。

スマート カードの電源投入時認証サポートの有効/無効の設定

このオプションを有効にすると、コンピュータの電源投入時のユーザ認証にスマート カードを使用できます。

注記：　電源投入時認証機能を完全に有効にするには、Java Card Security for HP ProtectTools モジュールを使用してスマート カードも設定する必要があります。

スマート カードの電源投入時認証サポートを有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]** をクリックします。
4. 左側のパネルで、**[Security]**（セキュリティ）をクリックします。
5. **[Smart Card Security]**（スマート カード セキュリティ）で、**[Enable]**（有効にする）をクリックします。

   注記：　スマート カード電源投入時認証を無効にするには、**[Disable]**（無効にする）をクリックします。

6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

内蔵セキュリティの電源投入時認証サポートの有効/無効の設定

このオプションを有効にすると、TPM 内蔵セキュリティ チップ（使用可能な場合のみ）をコンピュータの電源投入時のユーザ認証に使用できます。

注記： 電源投入時認証機能を完全に有効にするには、Embedded Security for HP ProtectTools モジュールを使用して TPM 内蔵セキュリティ チップも設定する必要があります。

内蔵セキュリティの電源投入時認証サポートを有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。
4. 左側のパネルで、**[Security]**（セキュリティ）をクリックします。
5. **[Embedded Security]**（内蔵セキュリティ）で、**[Power-on Authentication Support]**（電源投入時認証サポート）の隣の**[Enable]**（有効にする）をクリックします。

   注記： 内蔵セキュリティの電源投入時認証を無効にするには、**[Disable]**（無効にする）をクリックします。
6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

自動 DriveLock によるハードドライブのプロテクトの有効/無効の設定

このオプションが有効になっていると、DriveLock パスワードがドライブ内で自動的に生成および設定され、TPM 内蔵セキュリティ チップによって保護されます。

注記： コンピュータを再起動し、パスワードの入力画面で正しい TPM 内蔵セキュリティ パスワードを入力するまでは、自動的に生成されたパスワードは設定されません。

自動 DriveLock を有効にするオプションは、コンピュータに TPM セキュリティ チップが内蔵され初期化されており、かつ有効な DriveLock パスワードがない場合にのみ利用できます。 TPM セキュリティ チップを有効にして初期化する手順については、34 ページの 「内蔵セキュリティ チップの有効化」および35 ページの 「内蔵セキュリティ チップの初期化」を参照してください。

注記： コンピュータに DriveLock パスワードがすでに手動で設定されている場合は、自動 DriveLock によるプロテクトを有効にする前に、まず設定されているパスワードを無効にする必要があります。

自動 DriveLock によるプロテクトを有効または無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。
4. 左側のパネルで、**[Security]**（セキュリティ）をクリックします。
5. **[Embedded Security]**（内蔵セキュリティ）で、**[Automatic DriveLock Suport]**（自動ドライブロック サポート）の隣の**[Enable]**（有効にする）をクリックします。

   注記： Embedded Security の自動 DriveLock プロテクトを無効にするには、**[Disable]**（無効にする）をクリックします。

6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

[Computer Setup]のパスワードの管理

BIOS Configuration を使用すると、[Computer Setup]の電源投入時パスワードやセットアップ パスワードの設定および変更を行うことができるほか、各種のパスワード設定も管理できます。

注意： BIOS Configuration の[Passwords]（パスワード）ページで設定したパスワードは、[HP ProtectTools]ウィンドウの**[Apply]**（適用）または**[OK]**ボタンをクリックすると直ちに保存されます。 パスワード設定を元に戻す場合も以前のパスワードを指定する必要があるため、設定したパスワードを忘れないようにしてください。

電源投入時パスワードは、ノートブック コンピュータを不正な使用から保護できます。

注記： 電源投入時パスワードを設定すると、[Passwords]ページの[Set]（設定）ボタンが[Change]（変更）ボタンに置き換えられます。

[Computer Setup]のパスワードは、[Computer Setup]内の設定値とシステム識別情報を保護します。いったんこのパスワードを設定すると、次回から[Computer Setup]へのアクセスにはこのパスワード

の使用が必要になります。 セットアップ パスワードを設定している場合は、HP ProtectTools の BIOS Configuration の部分を起動する前にパスワードを入力するよう要求されます。

注記： セットアップ パスワードを設定すると、[Passwords]ページの[Set]ボタンが[Change]ボタンに置き換えられます。

電源投入時パスワードの設定

電源投入時パスワードを設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Power-On Password]**（電源投入時パスワード）の隣の**[Set]**（設定）をクリックします。
4. **[Enter Password]**（パスワードの入力）および**[Verify Password]**（パスワードの確認）ボックスにパスワードを入力して確定します。
5. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

電源投入時パスワードの変更

電源投入時パスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Power-On Password]**（電源投入時パスワード）の隣の**[Change]**（変更）をクリックします。
4. **[Old Password]**（古いパスワード）ボックスに、現在のパスワードを入力します。
5. **[Enter New Password]**（新しいパスワードの入力）ボックスに新しいパスワードを設定して確定します。
6. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
7. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

セットアップ パスワードの設定

[Computer Setup]のパスワードを設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。

3. 右側のパネルで、**[Setup Password]**（セットアップ パスワード）の隣の**[Set]**（設定）を選択します。
4. **[Enter Password]**（パスワードの入力）および**[Confirm Password]**（パスワードの確認）ボックスにパスワードを設定して確定します。
5. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

セットアップ パスワードの変更

[Computer Setup]のパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Setup Password]**（セットアップ パスワード）の隣の**[Change]**（変更）をクリックします。
4. **[Old Password]**（古いパスワード）ボックスに、現在のパスワードを入力します。
5. **[Enter New Password]**（新しいパスワードの入力）および**[Verify new password]**（新しいパスワードの確認）ボックスに新しいパスワードを入力して確定します。
6. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
7. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

パスワード オプションの設定

BIOS Configuration for HP ProtectTools を使用すると、システムのセキュリティを強化するようにパスワード オプションを設定できます。

厳重なセキュリティの有効化および無効化

注意： コンピュータが永久に使用できなくなることを防ぐため、設定したセットアップ パスワード、電源投入時パスワード、またはスマート カードの PIN を、紙などに書いて他人の目にふれない安全な場所に保管しておいてください。 これらのパスワードや PIN を忘れてしまうと、コンピュータのロックを解除できなくなります。

厳重なセキュリティを有効にすると、電源投入時パスワード、管理者パスワード、およびその他の電源投入時認証形式による保護が強化されます。

厳重なセキュリティを有効または無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルの**[Password options]**（パスワード オプション）で、**[Stringent Security]**（厳重なセキュリティ）を有効または無効にします。

注記： 厳重なセキュリティを無効にする場合は、**[Enable Stringent Security]**（厳重なセキュリティの有効化）チェック ボックスのチェックを外します。

4. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

Windows 再起動時の電源投入時認証の有効/無効の設定

このオプションを使用すると、Windows の再起動時にユーザに電源投入時、TPM、またはスマートカードの各パスワードの入力を要求することでセキュリティを強化できます。

Windows の再起動時の電源投入時認証を有効または無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルの**[Password options]**（パスワード オプション）で、**[Require password on restart]**（再起動時のパスワードの要求）を有効または無効にします。
4. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

6 Device Access Manager for HP ProtectTools

このセキュリティ ツールは、管理者だけが使用できます。 Device Access Manager for HP ProtectTools は、コンピュータ システムに取り付けられたデバイスを不正なアクセスから保護する次のセキュリティ機能を備えています。

- デバイス アクセスを定義するためにユーザごとに作成されるデバイス プロファイル
- グループ メンバーシップに基づいて許可または拒否可能なデバイス アクセス制御

バックグラウンド サービスの開始

デバイス プロファイルを適用するには、HP ProtectTools Device Locking/Auditing（HP ProtectTools デバイス ロック/検査）バックグラウンド サービスが実行されている必要があります。 初めてデバイス プロファイルの適用を試みると、HP ProtectTools セキュリティ マネージャにより、バックグラウンド サービスを開始するかどうかを尋ねるダイアログ ボックスが表示されます。 バックグラウンド サービスを開始し、またシステムが起動するたびに自動的に起動するように設定するには、**[Yes]**（はい）をクリックします。

簡易構成

この機能を使用して、次のクラスのデバイスへのアクセスを拒否できます。

- 管理者以外のユーザによるすべての USB デバイス
- 管理者以外のユーザによるすべてのリムーバブル メディア（フロッピーディスク、USB メモリなど）
- 管理者以外のユーザによるすべての DVD/CD-ROM ドライブ
- 管理者以外のユーザによるすべてのシリアル ポートおよびパラレル ポート

管理者以外のすべてのユーザによるデバイス クラスへのアクセスを拒否するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Simple Configuration]**（簡易構成）の順にクリックします。
3. 右側のパネルで、アクセスを拒否するデバイスのチェック ボックスにチェックを入れます。
4. **[Apply]**（適用）をクリックします。

   注記： バックグラウンド サービスが実行されていない場合は、ここで起動が試みられます。 **[Yes]**（はい）をクリックして許可します。

5. **[OK]**をクリックします。

デバイス クラス構成（詳細設定）

特定のユーザまたはユーザ グループによる、特定の種類のデバイスへのアクセスを許可または拒否するための選択項目も利用できます。

ユーザまたはグループの追加

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. **[Add]**（追加）をクリックします。 **[Select Users or Groups]**（ユーザまたはグループの選択）ダイアログ ボックスが表示されます。
5. **[Advanced]**（詳細）→**[Find Now]**（今すぐ検索）の順に選択して、追加するユーザまたはグループを検索します。
6. 使用可能なユーザおよびグループの一覧に追加するユーザまたはグループをクリックして**[OK]**をクリックします。
7. **[OK]**をクリックします。

ユーザまたはグループの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. 削除するユーザまたはグループをクリックして**[Remove]**（削除）をクリックします。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。

ユーザまたはグループのアクセス拒否

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. **[User/Groups]**（ユーザ/グループ）で、アクセスを拒否するユーザまたはグループをクリックします。
5. アクセスを拒否するユーザまたはグループの隣の**[Deny]**（拒否）をクリックします。
6. **[Apply]**（適用）→**[OK]**の順にクリックします。

グループの単一ユーザによるデバイス クラスへのアクセス許可

単一のユーザによるデバイス クラスへのアクセスを許可し、そのユーザのグループのその他のメンバーによるアクセスは拒否するように設定できます。

単一のユーザによるアクセスは許可し、グループには許可しないように設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. **[User/Groups]**（ユーザ/グループ）で、アクセスを拒否するグループを追加します。
5. アクセスを拒否するグループの隣の**[Deny]**（拒否）をクリックします。
6. 目的のクラスの下のフォルダに移動し、特定のユーザを追加します。 **[Allow]**（許可）をクリックして、そのユーザによるアクセスを許可します。
7. **[Apply]**（適用）→**[OK]**の順にクリックします。

グループの単一ユーザによる特定のデバイスへのアクセス許可

単一のユーザによる特定のデバイスへのアクセスを許可し、そのユーザのグループのその他のメンバーによる、クラス内のすべてのデバイスへのアクセスは拒否するように設定できます。

特定のデバイスへのアクセスを単一のユーザには許可し、グループには許可しないように設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックして、その下のフォルダに移動します。
4. **[User/Groups]**（ユーザ/グループ）で、アクセスを拒否するグループを追加します。
5. アクセスを拒否するグループの隣の**[Deny]**（拒否）をクリックします。
6. デバイスの一覧で、ユーザによるアクセスを許可する特定のデバイスに移動します。
7. **[Add]**（追加）をクリックします。 **[Select Users or Groups]**（ユーザまたはグループの選択）ダイアログ ボックスが表示されます。
8. **[Advanced]**（詳細）→**[Find Now]**（今すぐ検索）の順に選択して、追加するユーザまたはグループを検索します。
9. アクセスを許可するユーザをクリックして**[OK]**をクリックします。
10. **[Allow]**（許可）をクリックして、そのユーザによるアクセスを許可します。
11. **[Apply]**（適用）→**[OK]**の順にクリックします。

7 Drive Encryption for HP ProtectTools

注意： Drive Encryption モジュールをアンインストールする場合は、まず、暗号化されたすべてのドライブの暗号化を解除する必要があります。 そうしないと、Drive Encryption 復元サービスに登録していない限り、暗号化されたドライブ上のデータにアクセスできなくなります（69 ページの 「復元」を参照してください）。 Drive Encryption モジュールを再インストールしても、暗号化されたドライブにはアクセスできません。

暗号化の管理

ドライブの暗号化

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Encryption Management]**（暗号化の管理）の順にクリックします。
3. 右側のパネルで、**[Activate]**（有効にする）をクリックします。 [Drive Encryption for HP ProtectTools Wizard]（Drive Encryption for HP ProtectTools ウィザード）が起動します。
4. 画面の説明に沿って操作し、暗号化を有効にします。

注記： リカバリ情報を保存するためのフロッピーディスク、フラッシュ ストレージ デバイス、またはその他の USB 接続ストレージ メディアを指定する必要があります。

暗号化の変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Encryption Management]**（暗号化の管理）の順にクリックします。
3. 右側のパネルで、**[Change encryption]**（暗号化の変更）をクリックします。 **[Change Encryption]**（暗号化の変更）ダイアログ ボックスで、暗号化するディスクを選択して**[OK]**をクリックします。
4. **[OK]**を再度クリックして、暗号化を開始します。

デバイスの暗号化解除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Encryption Management]**（暗号化の管理）の順にクリックします。
3. 右側のパネルで、**[Deactivate]**（無効にする）をクリックします。

ユーザ管理

ユーザの追加

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[User Management]**（ユーザ管理）の順にクリックします。
3. 右側のパネルで、**[Add]**（追加）をクリックします。**[User Name]**（ユーザ名）リストのユーザ名をクリックするか、または**[Username]**（ユーザ名）ボックスにユーザ名を入力します。**[Next]**（次へ）をクリックします。
4. 選択したユーザの Windows パスワードを入力して**[Next]**（次へ）をクリックします。
5. 新しいユーザの認証方法を選択して**[Finish]**（完了）をクリックします。

ユーザの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[User Management]**（ユーザ管理）の順にクリックします。
3. 右側のパネルで、**[User Name]**（ユーザ名）リストから削除するユーザ名をクリックします。**[Remove]**（削除）をクリックします。
4. **[Yes]**（はい）をクリックして、選択したユーザの削除を確定します。

トークンの変更

ユーザの認証方法を変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[User Management]**（ユーザ管理）の順にクリックします。
3. 右側のパネルで、**[User Name]**（ユーザ名）リストからユーザ名を選択して**[Change Token]**（トークンの変更）をクリックします。
4. ユーザの Windows パスワードを入力して**[Next]**（次へ）をクリックします。
5. 新しい認証方法を選択して**[Finish]**（完了）をクリックします。
6. 認証方法として Java Card を選択した場合は、入力を要求されたら Java Card のパスワードを入力して**[OK]**をクリックします。

パスワードの設定

パスワードの設定、またはユーザの認証方法の変更を行うには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[User Management]**（ユーザ管理）の順にクリックします。
3. 右側のパネルで、**[User Name]**（ユーザ名）リストからユーザを選択して**[Set Password]**（パスワードの設定）をクリックします。
4. ユーザの Windows パスワードを入力して**[Next]**（次へ）をクリックします。
5. 新しい認証方法を選択して**[Finish]**（完了）をクリックします。
6. 認証方法として Java Card を選択した場合は、入力を要求されたら Java Card のパスワードを入力して**[OK]**をクリックします。

復元

使用可能な安全策として、次の 2 つがあります。

- パスワードを忘れた場合は、暗号化されたドライブにアクセスできません。 ただし、Drive Encryption 復元サービスに登録しておくと、パスワードを忘れた場合でもコンピュータにアクセスできるようになります。
- Drive Encryption キーを、フロッピーディスク、フラッシュ ストレージ デバイス、またはその他の USB 接続ストレージ メディアにバックアップできます。

Drive Encryption 復元サービスへの登録

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Recovery]**（リカバリ）の順にクリックします。
3. 右側のパネルで、**[Click here to register]**（登録するにはここをクリック）をクリックします。要求された情報を入力して、セキュリティ バックアップ手順を完了します。

Drive Encryption キーのバックアップ

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Recovery]**（リカバリ）の順にクリックします。
3. 右側のパネルで、**[Click here to backup your keys]**（キーをバックアップするにはここをクリック）をクリックします。
4. リカバリ情報を保存するフロッピーディスク、フラッシュ ストレージ デバイス、またはその他の USB 接続ストレージ メディアを選択して**[Next]**（次へ）をクリックします。 [Drive Encryption for HP ProtectTools Wizard]（Drive Encryption for HP ProtectTools ウィザード）が起動します。
5. 画面の説明に沿って操作し、Drive Encryption キーをバックアップします。

注記： リカバリ情報を保存するためのフロッピーディスク、フラッシュ ストレージ デバイス、またはその他の USB 接続ストレージ メディアを指定する必要があります。

8 トラブルシューティング

Credential Manager for HP ProtectTools

簡単な説明	詳しい説明	解決方法
Credential Manager の **[Network Accounts]**（ネットワーク アカウント）オプションを使用すると、ユーザはログオン先のドメイン アカウントを選択できる。 TPM 認証が使用されている場合は、このオプションを使用できない。 他の認証方法はすべて正しく機能する	TPM 認証を使用している場合、ユーザはローカル コンピュータにのみログオンされます	Credential Manager の[シングルサインオン]ツールを使用すると、ユーザは他のアカウントを認証できるようになります
Windows XP Service Pack 1 へのログオンで、USB トークン証明情報を使用できない	USB トークン ソフトウェアをインストールし、USB トークン証明情報を登録して、Credential Manager をプライマリ ログオンとして設定すると、USB トークンは Credential Manager/GINA のログオンに表示されず、使用できません Windows にログオンしなおし、Credential Manager からログオフした後、Credential Manager に再度ログオンしトークンをプライマリ ログオンとして再選択すると、トークンのログオン操作が正常に機能します	Windows Update を使用して、Windows を Service Pack 2 にアップデートしてください Service Pack 1 を使用し続ける場合は、ログオフのために別の証明情報（Windows パスワード）を使用して Windows にログオンしなおし、Credential Manager に再度ログオンしてください
一部のアプリケーションの Web ページでエラーが発生し、ユーザがタスクを実行または完了できなくなる	シングルサインオンの機能無効化パターンにより、一部の Web ベースのアプリケーションが機能を停止し、エラーを報告します。 たとえば、Internet Explorer では黄色い三角形の中に**[!]**が表示され、エラーの発生を通知します	Credential Manager シングルサインオンは、すべてのソフトウェアの Web インタフェースをサポートしているわけではありません。 シングルサインオンのサポートをオフにすることにより、特定の Web ページに対するシングルサインオンのサポートを無効にしてください。 Credential Manager のヘルプ ファイルに含まれている、シングルサインオンに関する詳しいドキュメントを参照してください 特定のアプリケーションで特定のシングルサインオンを無効にできない場合は、HP のサポート窓口にお問い合わせください
ログオン プロセス中に、**[Browse for Virtual Token]**（仮想トークンの参照）のオプションが表示されない	セキュリティ上のリスクを軽減するために参照のオプションが削除されたため、Credential Manager で、ユーザは登録された仮想トークンの場所を移動できません	参照のオプションは、ユーザ以外の利用者がファイルを削除したり、ファイルの名前を変更したりして Windows を制御できてしまうため、削除されました

簡単な説明	詳しい説明	解決方法
権限がある場合でも、ドメイン管理者が Windows パスワードを変更できない	これは、ドメイン管理者がドメインにログオンし、ドメインとローカル コンピュータで管理者の権限をもつアカウントを使用して、ドメイン ID を Credential Manager に登録した後で発生します。ドメイン管理者が、Credential Manager から Windows のパスワードを変更しようとすると、ログオンの失敗を示す次のようなエラー メッセージが表示されます。**[User account restriction]**（ユーザ アカウントの制限）	Credential Manager では、**[Change Windows password]**（Windows パスワードの変更）を使用してドメイン ユーザのアカウント パスワードを変更することはできません。 Credential Manager では、ローカル コンピュータのアカウント パスワードのみ変更可能です。 ドメイン ユーザは、**[Windows Security]**（Windows セキュリティ）→**[Change password]**（パスワードの変更）オプションを使用して自分のパスワードを変更できますが、ドメイン ユーザはローカル コンピュータ上に物理アカウントを持っていないため、Credential Manager はログオンに使用されたパスワードしか変更できません
Credential Manager に、Corel WordPerfect 12 のパスワード GINA との非互換性の問題がある	ユーザが Credential Manager にログオンし、WordPerfect でドキュメントを作成して、パスワード保護を使用して保存した場合、Credential Manager は、パスワード GINA を（手動または自動にかかわらず）検出または認識することができません	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Credential Manager が画面の**[Connect]**（接続）ボタンを認識しない	シングルサインオンが再起動されたときに、リモート デスクトップ接続（RDP）のシングルサインオン証明情報が**[Connect]**（接続）に設定されていると、**[Connect]**（接続）の代わりに常に**[Save As]**（名前を付けて保存）が入力されます	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
ユーザが、TPM で保護されている Credential Manager 証明情報をすべて失う場合がある	TPM モジュールが取り外されたり破損したりすると、TPM が保護する証明情報がすべて失われます	これは仕様です TPM モジュールは、Credential Manager 証明情報を保護するように設計されています。 TPM モジュールを取り外す前に、Credential Manager から ID をバックアップしておくことをおすすめします
Windows XP Service Pack 1 を使用している場合のみ、スリープ モードからハイバネーションに移行した後、Credential Manager にログオンできない	システムがハイバネーションやスリープ モードに移行すると、選択されているログオン証明情報の種類（パスワード、指紋、または Java Card）にかかわらず、管理者やユーザは Credential Manager にログオンできなくなり、Windows のログオン画面が表示されたままになります	Windows Update を使用して、Windows を Service Pack 2 にアップデートしてください。 この問題の原因について詳しくは、http://www.microsoft.com/japan/ にあるマイクロソフト サポート技術情報の文書番号 813301 を参照してください ユーザがログオンするには、Credential Manager を選択してログオンする必要があります。 Credential Manager にログオンすると、Windows にログオンして（Windows ログオン オプションの選択が必要になる場合があります）ログオン プロセスを完了するよう要求されます ユーザが最初に Windows にログオンした場合は、手動で Credential Manager にログオンする必要があります
Embedded Security を復元すると、Credential Manager が機能しなくなる	ROM を工場出荷時の設定に復元した後は、Credential Manager が証明書を登録できなくなります	Credential Manager をインストールした後に ROM が工場出荷時の設定に戻されると、Credential Manager は TPM へのアクセスに失敗します TPM 内蔵セキュリティ チップは、f10 [Computer Setup]ユーティリティ、BIOS Configuration、または HP Client Manager を使用して有効にできます。

簡単な説明	詳しい説明	解決方法
		[Computer Setup]を使用して TPM 内蔵セキュリティチップを有効にするには、以下の手順で操作します 1. コンピュータの電源を入れるか再起動し、画面の左下隅に**[f10=ROM Based Setup]**メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します 2. 矢印キーを使用して、**[Security]**（セキュリティ設定）→**[Setup Password]**（セットアップ パスワード）の順に選択します。 パスワードを設定します 3. **[Embedded Security Device]**（内蔵セキュリティ デバイス）を選択します 4. 矢印キーを使用して、**[無効]**（Embedded Security Device–Disable）を選択します。矢印キーを使用して、**[有効]**（Embedded Security Device–Enable）に変更します 5. **[Enable]**（有効にする）→**[Save changes and exit]**（設定を保存して終了）の順に選択します HP では、将来のカスタマ ソフトウェア リリースに向けて、解決策を調査中です
セキュリティの**[Restore Identity]**（ID の復元）プロセスで、仮想トークンとの関連付けが失われる	ユーザが ID を復元したとき、Credential Manager で、ログオン画面での仮想トークンの場所との関連付けが失われる場合があります。 Credential Manager には仮想トークンが登録されているにもかかわらず、ユーザは関連付けを復元するためにトークンを再登録する必要があります	現在の仕様です ID を保存しないで Credential Manager をアンインストールすると、トークンのシステム（サーバ）の部分が破壊されるため、トークンのクライアントの部分が ID の復元によって復元されたとしても、そのトークンはログオンに使用できなくなります HP では、一時的ではない解決策を調査中です

Embedded Security for HP ProtectTools

簡単な説明	詳しい説明	解決方法
PSD 上のフォルダ、サブフォルダ、およびファイルを暗号化するとエラー メッセージが表示される	ユーザがファイルおよびフォルダを PSD にコピーし、フォルダ/ファイルまたはフォルダ/サブフォルダを暗号化しようとすると、**[Error Applying Attributes]**（属性適用時のエラー）というメッセージが表示されます。 C ドライブまたは外付けハードドライブ上では同じファイルを暗号化できます	これは仕様です ファイル/フォルダを PSD に移動すると、これらのファイル/フォルダは自動的に暗号化されます。 ファイル/フォルダを二重に暗号化する必要はありません。EFS を使用して PSD 上のファイル/フォルダを二重に暗号化しようとすると、このエラー メッセージが表示されます
マルチブート プラットフォーム環境で別の OS を使用して所有権を得ることができない	ドライブがマルチ OS ブート用にセットアップされている場合でも、所有権を設定できるのは、1 つのオペレーティング システムのプラットフォーム初期化ウィザードからだけです	これはセキュリティを確保するための仕様です
不正な管理者が、暗号化された EFS フォルダの内容の表示、削除、名前の変更、または移動を行うことができる	フォルダを暗号化している場合でも、管理権限がある不正なユーザは、フォルダの内容の表示、削除、または移動を行えます	これは仕様です これは、Embedded Security TPM ではなく EFS の機能です。Embedded Security は、Microsoft EFS ソフトウェアを使用し、EFS がすべての管理者のファイル/フォルダへのアクセス権限を保護します
FAT32 を使用したハードドライブを復元しようとするとき、ユーザに暗号化のオプションが表示されない	FAT32 を使用するハードディスク ドライブを復元する場合は、EFS を使用してファイル/フォルダを暗号化するオプションが表示されません	これは仕様です。 FAT32 パーティションを含む復元ディスクにはソフトウェアをインストールしないでください Microsoft EFS は NTFS でのみサポートされており、FAT32 では機能しません。これは Microsoft EFS の機能であり、HP ProtectTools ソフトウェアによるものではありません
ユーザがリカバリ アーカイブの XML ファイルを暗号化または削除できる	設計では、このフォルダに ACL は設定されていないため、ユーザがこのファイルを誤って、または意図的に暗号化または削除することによってアクセス不可能にする可能性があります。 このファイルが暗号化または削除されると、だれも TPM ソフトウェアを使用できなくなります	これは仕様です ユーザは、基本ユーザ キーのバックアップ コピーを保存または更新できるように、緊急アーカイブに対するアクセス権を持っています。 リカバリ アーカイブ ファイルを決して暗号化または削除しないようユーザに指示してください
Embedded Security EFS と Symantec Antivirus または Norton Antivirus との相互通信によって、暗号化/暗号化解除やスキャンの時間が長くなる	暗号化されたファイルは、Symantec Antivirus または Norton Antivirus 2005 のウィルス スキャンと干渉します。 スキャン プロセスの間、基本ユーザ パスワードの入力画面では、約 10 ファイルごとにパスワードを入力するよう求められます。 ユーザがパスワードを入力しないと、基本ユーザ パスワードの入力画面がタイムアウトし、Norton Antivirus 2005 によってスキャンが継続されます。 Symantec Antivirus または Norton Antivirus の実行中は、Embedded Security EFS を使用したファイルの暗号化には時間がかかります	Embedded Security EFS ファイルをスキャンするために必要な時間を短縮するために、ユーザはスキャンの前に暗号化パスワードを入力するか、またはスキャンの前に暗号化を解除することができます Embedded Security EFS を使用してデータを暗号化/暗号化解除するために必要な時間を短縮するには、Symantec Antivirus または Norton Antivirus で[Auto-Protect]（自動保護）を無効にしてください
緊急リカバリ アーカイブをリムーバブル メディアに保存できない	Embedded Security の初期化中、緊急リカバリ アーカイブのパスを作成しているときにユーザがマルチメディア カードまたは SD（Secure Digital）メモリ カードを挿入すると、エラー メッセージが表示されます	これは仕様です リムーバブル メディアへのリカバリ アーカイブの保存はサポートされていません。 リカバリ アーカイブは、ネットワーク ドライブか、または C ドライブ以外のローカル ドライブに保存できます

簡単な説明	詳しい説明	解決方法
電源の切断によってEmbedded Security の初期化が中断された後、エラーが発生する	Embedded Security チップの初期化中に電源が切断されると、次の問題が発生します ● [Embedded Security Initialization Wizard]（Embedded Security 初期化ウィザード）を起動しようとしたときに、次のエラー メッセージが表示されます。 **[The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner.]**（Embedded Security チップにすでにEmbedded Security 所有者が設定されているため、Embedded Security を初期化できません。） ● [User Initialization Wizard]（ユーザ初期化ウィザード）を起動しようとしたときに、次のエラー メッセージが表示されます。 **[The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.**（Embedded Security が初期化されていません。ウィザードを使用するには、まずEmbedded Security を初期化する必要があります。）	電源が切断された後は、以下の手順に従って回復します **注記：**　特別な指定がない場合、メニューやメニュー項目を選択したり、値を変更したりするには矢印キーを使用します 1. コンピュータを起動または再起動します 2. 画面に**[f10=Setup]**メッセージが表示されたら、f10 キーを押します 3. 該当する言語オプションを選択します 4. enter キーを押します 5. **[Security]**（セキュリティ設定）→**[Embedded Security]**（内蔵セキュリティ）の順に選択します 6. **[Embedded Security Device]**（内蔵セキュリティ デバイス）オプションを**[Enable]**（有効）に設定します 7. f10 キーを押して変更を確定します 8. **[File]**（ファイル）→**[Save Changes and Exit]**（設定を保存して終了）の順に選択します 9. enter キーを押します 10. f10 キーを押して変更を保存し、ユーティリティを終了します
TPM モジュールを有効にした後、[Computer Setup]（f10）ユーティリティのパスワードを削除できる	TPM モジュールを有効にするには、[Computer Setup]（f10）ユーティリティのパスワードが必要です。 モジュールを有効にしたら、ユーザはパスワードを削除することができます。 これにより、システムに直接アクセスできるユーザが TPM モジュールをリセットできると同時に、データが損失する可能性も発生します	これは仕様です [Computer Setup]（f10）ユーティリティのパスワードは、そのパスワードを知っているユーザだけが削除できます。 それでも、[Computer Setup]（f10）ユーティリティのパスワードを常に保護しておくことを強くおすすめします
スタンバイ状態の後にシステムがアクティブになったとき、Personal Secure Drive（PSD）のパスワード ボックスが表示されない	PSD を作成した後にユーザがシステムにログオンすると、TPM から基本ユーザ パスワードを入力するよう求められます。 ユーザがパスワードを入力しないうちにシステムのスタンバイが起動された場合、スタンバイから復帰してもパスワード ダイアログ ボックスは表示されません	これは仕様です ユーザがいったんログオフしてからログオンすれば、PSD パスワード ボックスは表示されます
セキュリティ プラットフォーム ポリシーを変更するときにパスワードを要求されない	セキュリティ プラットフォーム ポリシーへのアクセス（マシンとユーザの両方）では、システムの管理権限を持っているユーザは、TPM パスワードの入力を要求されません	これは仕様です TPM ユーザが初期化されている場合でもされていない場合でも、管理者であればセキュリティ プラットフォーム ポリシーを変更できます
証明書を表示すると、信頼されていないものとして表示される	HP ProtectTools をセットアップし、[User Initialization Wizard]（ユーザ初期化ウィザード）を実行した後、ユーザは発行した証明書を表示することができま	自己署名の証明書は、信頼されません。正しく設定された企業環境では、EFS の証明書は、オンラインの証明機関が発行し、信頼されます

簡単な説明	詳しい説明	解決方法
	す。ただし、証明書を表示すると、信頼されていないものとして表示されます。 インストール ボタンをクリックすることによって、この時点で証明書をインストールできますが、インストールしても信頼される証明書にはなりません	
次の断続的な暗号化および暗号化解除エラーが発生する。 **[The process cannot access the file because it is being used by another process.]**（別のプロセスでファイルが使用されているため、現在のプロセスからはこのファイルにアクセスできません。）	これは、ファイルの暗号化または暗号化解除を行うときに発生する、きわめて断続的なエラーです。そのファイルまたはフォルダがオペレーティング システムやその他のアプリケーションによって処理されていない場合でも、ファイルが別のプロセスによって使用されているために発生します	この問題を解決するには、次の手順で操作します **1.** システムを再起動します **2.** ログオフします **3.** ログオンしなおします
新しいデータの生成または転送が完了する前にリムーバブル メディアを取り外すと、リムーバブル メディア内のデータが損失する	マルチベイ ハードドライブなどのストレージ メディアを取り外しても、Personal Secure Drive（PSD）は引き続き使用可能と表示され、PSD にデータを追加/変更している間もエラーは生成されません。 システムが再起動された後、PSD には、リムーバブル記憶域が使用不可の間に発生したファイル変更が反映されません	データの生成または転送が完了する前に PSD を取り外さないでください。 この問題は、ユーザが PSD にアクセスした後、新しいデータの生成または転送が完了する前にハードドライブを取り外した場合にのみ発生します。 リムーバブル ハードドライブが存在しないときにユーザが PSD にアクセスしようとすると、**[the device is not ready]**（デバイスの準備ができていません）というエラー メッセージが表示されます
アンインストール中、基本ユーザを初期化しないで管理ツールを開くと、**[Disable]**（無効にする）オプションが使用できず、管理ツールが閉じられるまでアンインストーラの処理が続行されない	ユーザは、TPM を無効にしないでアンインストールするか、または最初に（管理ツールを使用して）TPM を無効にしてからアンインストールするかのどちらかを選択できます。 管理ツールにアクセスするには、基本ユーザ キーの初期化が必要です。 基本ユーザの初期化が実行されていないと、すべてのオプションがアクセス不可になります **[Click Yes to open Embedded Security Administration tool]**（Embedded Security 管理ツールを開くには[Yes]（はい）をクリックしてください）ダイアログ ボックスで**[Yes]**（はい）をクリックすることによって、管理ツールを開くことを明示的に選択しているため、アンインストールは管理ツールが閉じられるまで行われません。 そのダイアログ ボックスで**[No]**（いいえ）をクリックした場合、管理ツールはまったく開かれず、アンインストールの処理が続行されます	管理ツールは TPM チップを無効にするために使用されますが、基本ユーザ キーがすでに初期化されていない限り、そのオプションは使用できません。 基本ユーザ キーがまだ初期化されていない場合は、**[OK]**または**[Cancel]**（キャンセル）を選択してアンインストールを続行してください
2 つのユーザ アカウントに PSD を作成し、128 MB のシステム構成でユーザの簡易切り替えを使用した後、断続的にシステムがロックアップする	最小の RAM で簡易切り替えを使用していると、[ようこそ]（ログオン）画面の代わりに黒い画面が表示され、キーボードやマウスの応答がない状態でシステムがロックアップする可能性があります	根本的な原因は、少ないメモリ構成でのタイミングの問題と考えられます 内蔵グラフィックスは、8 MB のメモリが必要な UMA アーキテクチャを採用しているため、ユーザに使用可能なメモリは 120 MB しか残されません。 ともにログオンし、ユーザの簡易切り替えを行っている両方のユーザがこの 120 MB を共有すると、このエラーが発生します

簡単な説明	詳しい説明	解決方法
		エラーを回避するには、システムを再起動し、メモリ構成を増やしてください（HP ではセキュリティ モジュール搭載の 128 MB 構成コンピュータを出荷していません）
[access denied]（アクセスが拒否されました）というメッセージが表示され、EFS ユーザ認証（パスワード要求）がタイムアウトする	**[OK]**をクリックするか、またはスタンバイが終了した後、EFS ユーザ認証のパスワード画面が再度開きます	これは仕様です。Microsoft EFS で問題が発生しないように、エラー メッセージを生成するために 30 秒程度のウォッチドッグ タイマーが作成されました
日本語でのセットアップ中に、機能説明が省略されることがある	インストール ウィザード実行時のカスタム セットアップ オプション段階で、機能説明が省略されています	この問題については、将来のリリースで解決します
入力画面にパスワードを入力しなくても、EFS 暗号化が機能する	ユーザ パスワードの入力画面でタイムアウトが可能なため、ファイルまたはフォルダに対して引き続き暗号化を使用できます	暗号化の機能は、Microsoft EFS 暗号化の機能であるため、パスワード認証は必要ありません。 暗号化の解除には、ユーザ パスワードの指定が必要になります
[User Initialization Wizard]（ユーザ初期化ウィザード）で電子メールのセキュリティ保護を指定しない場合、またはユーザ ポリシーで電子メールのセキュリティ保護の設定が無効になっている場合でも、電子メールのセキュリティ保護がサポートされる	Embedded Security ソフトウェアやウィザードは、電子メール クライアント（Outlook、Outlook Express、または Netscape）の設定を制御しません	この動作は仕様です。 TPM の電子メール設定によって、電子メール クライアントで暗号化の設定を直接編集することは禁止されません。 電子メールのセキュリティ保護の使用は、他社製のアプリケーションによって設定および制御されます。 HP のウィザードでは、すばやいカスタマイズを可能にするため、3 つの参照アプリケーションにリンクできるようにしています
同じコンピュータまたは以前に初期化したコンピュータで 2 回目の大規模な導入を実行すると、緊急リカバリ ファイルおよび緊急トークン ファイルが上書きされる。新しいファイルは、リカバリに使用できない	以前に初期化された HP ProtectTools Embedded Security システムで大規模な導入を実行すると、XML ファイルが上書きされるため、既存のリカバリ アーカイブおよびリカバリ トークンが使用できなくなります	HP では、XML ファイルの上書きの問題を解決するよう取り組んでおり、将来の SoftPaq で解決策を提供する予定です
Embedded Security でのユーザ復元中に、自動化されたログオン スクリプトが機能しない	このエラーは、ユーザが次の操作を行った後に発生します • Embedded Security で、所有者とユーザを初期化する（初期設定の位置の**[マイ ドキュメント]**を使用） • BIOS で、チップを工場出荷時の設定に戻す • コンピュータを再起動する • Embedded Security の復元を開始する。 復元処理中、Credential Manager により、Infineon TPM ユーザ認証へのログオンを自動化するかどうか尋ねられます。 **[Yes]**（はい）を選択すると、SPEmRecToken の場所がテキスト ボックスに自動的に表示されます	画面の**[Browse]**（参照）ボタンをクリックして位置を選択してください。復元プロセスが続行されます

簡単な説明	詳しい説明	解決方法
	この位置が正しい場合でも、次のエラー メッセージが表示されます。**[No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.]**（緊急リカバリ トークンが入力されていません。緊急リカバリ トークンの取得元にするトークン位置を選択してください。）	
ユーザの簡易切り替えの環境で、複数ユーザの PSD が機能しない	このエラーは、複数のユーザが作成され、同じドライブ文字を含む Personal Secure Drive（PSD）が与えられている場合に発生します。 PSD がロードされたときにユーザ間でユーザの簡易切り替えを行おうとすると、2 番目のユーザの PSD が使用できなくなります	2 番目のユーザの PSD は、別のドライブ文字を使用するように設定しなおすか、または最初のユーザがログオフした場合にのみ使用可能になります
Personal Secure Drive（PSD）が生成されたハードドライブをフォーマットすると、PSD が無効になり、削除できなくなる	PSD のアイコンは引き続き表示されますが、ユーザが PSD にアクセスしようとすると、**[drive is not accessible]**（ドライブにアクセスできません）というエラー メッセージが表示されます ユーザは PSD を削除できず、次のメッセージが表示されます。 **[your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process]**（PSD はまだ使用されています。この PSD に開かれたままのファイルがなく、別のプロセスからもアクセスされていないことを確認してください） この PSD を削除するには、ユーザはシステムをリブートする必要があります。リブートの後、PSD はロードされません	これは仕様です。ユーザが強制的に削除したり、PSD データの保存位置から切断したりしても、Embedded Security PSD ドライブ エミュレーションが機能を続行し、存在しないデータとの通信が途切れるため、エラーが生成されます 解決策：次の再起動後はエミュレーションがロードされないため、ユーザは古い PSD エミュレーションを削除して、新しい PSD を作成できます
ユーザが自動バックアップ アーカイブから復元しているときに内部エラーが検出される	Embedded Security では、自動バックアップ アーカイブから復元するために **[Restore under Backup]**（バックアップの復元）オプションをクリックし、**[SPSystemBackup.xml]**を選択すると、復元ウィザードの実行に失敗して次のエラー メッセージが表示されます。**[The selected Backup Archive does not match the restore reason. Please select another archive and continue.]**（選択されたバックアップ アーカイブは復元の理由に一致しません。別のアーカイブを選択して続行してください。）	SpBackupArchive.xml が必要なときに **[SpSystemBackup.xml]**を選択すると、Embedded Security ウィザードの実行に失敗して次のメッセージが表示されます。 **[An internal Embedded Security error has been detected.]**（Embedded Security の内部エラーが検出されました。） 必要な理由に一致する正しい XML ファイルを選択する必要があります プロセスは設計どおりに正しく機能していますが、Embedded Security 内部エラー メッセージが明確でないため、より適切なメッセージを表示する必要があります。HP は、将来の製品で改善するよう取り組んでいます
セキュリティ システムで、複数のユーザでの復元エラーが発生する	復元プロセス中、管理者が復元するユーザを選択した場合、選択されなかったユーザが後で復元を試みてもキーを復元できません。**[decryption process failed]**（暗号化の解除プロセスが失敗しました）というエラー メッセージが表示されます	選択されなかったユーザは、初期設定による次回の日次バックアップが実行される前に、TPM をリセットし、復元プロセスを実行して、すべてのユーザを選択することによって復元できます。 自動化されたバックアップが実行された場合は、復元されなかったユーザが上書きされ、それらのユーザのデータは失われます。 新しいシステム バックアップ データが保存されると、選択されなかった以前のユーザは復元できなくなります

簡単な説明	詳しい説明	解決方法
		また、ユーザがシステム全体のバックアップを復元することも必要です。 アーカイブ バックアップは個別に復元できます
システム ROM を初期設定に戻すと、TPM が表示されなくなる	システム ROM を初期設定に戻すと、Windows が TPM を認識できなくなります。これより、セキュリティ ソフトウェアが正しく動作しなくなり、TPM の暗号化データにアクセスできなくなります	以下の手順に従って、BIOS で TPM を再表示します [Computer Setup]（f10）ユーティリティを開き、**[Security]**（セキュリティ設定）→**[Device security]**（デバイス セキュリティ）の順に選択して、フィールドを**[Hidden]**（非表示）から**[Available]**（利用可能）に変更します
マップされたドライブで自動バックアップが機能しない	管理者が Embedded Security で自動バックアップをセットアップすると、Windows XP の**[スタート]**→**[コントロール パネル]**→**[パフォーマンスとメンテナンス]**→**[タスク]**→**[タスク名]**にエントリが作成されます。 この**[タスク名]**は、バックアップを実行するためのアクセス権として NT AUTHORITY\SYSTEM を使用するように設定されています。 この設定はどのローカル ドライブに対しても正しく機能します 管理者が、自動バックアップでマップされたドライブに保存されるように設定すると、NT AUTHORITY\SYSTEM にはマップされたドライブを使用する権限がないため、プロセスは失敗します 自動バックアップをログオン時に実行するようにスケジュールが設定されている場合は、Embedded Security の TNA アイコンに次のメッセージが表示されます。 **[The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.]**（バックアップ アーカイブの場所に現在アクセスできません。バックアップ アーカイブが再びアクセス可能になるまで一時的なアーカイブにバックアップする場合は、ここをクリックしてください。）ただし、自動バックアップが特定の時間にスケジュール設定されている場合は、失敗の通知が表示されることなくバックアップが失敗します	この問題を回避するには、NT AUTHORITY\SYSTEM を[コンピュータ名]\[管理者名]に変更してください。これは、スケジュールされたタスクが手動で作成される場合の初期設定です HP では、[コンピュータ名]\[管理者名]を含む初期設定を備える製品を将来リリースできるよう取り組みを進めています
Embedded Security の GUI で Embedded Security を一時的に無効にできない	最新の 4.0 ソフトウェアは、HP Notebook 1.1B への実装と、HP Desktop 1.2 への実装をサポートすることを目的にして設計されました 無効化のためのこのオプションは、TPM 1.1 プラットフォームのソフトウェア インタフェースでもサポートされています	この問題については、将来のリリースで対応します

Device Access Manager for HP ProtectTools

簡単な説明	詳しい説明	解決方法
Device Access Manager 内でユーザがデバイスへのアクセスを拒否されたが、これらのデバイスは引き続きアクセス可能である	ユーザによるデバイスへのアクセスを拒否するために、Device Access Manager 内では簡易構成やデバイス クラス構成が使用されてきました。 アクセスを拒否されたにもかかわらず、ユーザは引き続きデバイスにアクセスできます	HP ProtectTools デバイス ロック サービスが開始していることを確認してください 管理者権限のあるユーザとしてログインし、**[コントロール パネル]**→**[管理ツール]**→**[サービス]**の順に選択します。 **[サービス]**ウィンドウで、**[HP ProtectTools Device Locking/Auditing]**サービスを見つけます。 このサービスが開始されおり、スタートアップの種類が**[自動]**であることを確認してください
ユーザがデバイスへの予期しないアクセスを許可されているか、またはユーザがデバイスへのアクセスを予期せず拒否される	Device Access Manager は、一部のデバイスへのアクセスを拒否し、その他のデバイスへのアクセスを許可するために使用されてきました。 ユーザがシステムを使用中に、Device Access Manager によって拒否されていると思っていたデバイスにアクセスできたり、Device Access Manager によって許可されていると思っていたデバイスへのアクセスを拒否されたりすることがあります	ユーザのデバイス設定の調査には、Device Access Manager 内のデバイス クラス構成を使用してください **[Security Manager]**（セキュリティ マネージャ）→**[Device Access Manager]**→**[Device Class Configuration]**（デバイス クラス構成）の順に選択します。 [Device Class]（デバイス クラス）ツリーの各レベルを展開し、ユーザに該当する設定を確認します。 そのユーザに対して設定されている[Deny]（拒否）アクセス権、またはそのユーザがメンバになっている Windows グループ（たとえば、Users、Administrators など）があるかどうかを確認してください
許可と拒否のどちらが優先されるか	デバイス クラス構成内では、次の構成が設定されています ● [Allow]（許可）アクセス権は、ある Windows グループ（たとえば、BUILTIN\Administrators）に許可されています。一方、[Deny]（拒否）アクセス権は、デバイス クラス階層内の同じレベル（たとえば、DVD/CD-ROM ドライブ）にある別の Windows グループ（たとえば、BUILTIN\Users）に許可されています あるユーザがこの両方のグループのメンバ（たとえば管理者）である場合は、どちらが優先されますか	このユーザはデバイスへのアクセスを拒否されます。 拒否は許可より優先されます アクセスは、Windows でデバイスに対する有効なアクセス権が決定される方法に従って拒否されます。 あるグループが拒否され、別のグループが許可されていますが、ユーザはこの両方のグループのメンバです。 アクセスの拒否はアクセスの許可より優先されるため、このユーザは拒否されます 回避策の 1 つは、DVD/CD-ROM ドライブのレベルにある Users グループを拒否し、DVD/CD-ROM ドライブより低いレベルにある Administrators グループを許可することです 別の回避策として、DVD/CD へのアクセスを許可するためと、DVD/CD へのアクセスを拒否するために別々の、特定の Windows グループを作成する方法もあります。 それから、該当するグループに特定のユーザを追加します

その他

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
セキュリティ マネージャ：次の警告が表示される。 **[The security application can not be installed until the HP Protect Tools Security Manager is installed.]**（HP ProtectTools セキュリティ マネージャがインストールされるまで、セキュリティ アプリケーションをインストールできません。）	Embedded Security、Java Card Security、指紋認証などのセキュリティ アプリケーションはすべて、セキュリティ マネージャ インタフェースの拡張可能なプラグインです。 HP が承認しているセキュリティ プラグインをロードするには、先にセキュリティ マネージャをインストールしておく必要があります	セキュリティ プラグインをインストールする前に、セキュリティ マネージャ ソフトウェアをインストールしておく必要があります
Broadcom に対応した TPM を含むモデルの TPM ファームウェア アップデート ユーティリティ：HP のサポート Web サイトから提供されたツールで **[ownership required]**（オーナシップが必要）と表示される	これは、Broadcom に対応した TPM を含むモデルの TPM ファームウェア ユーティリティの予期された動作です ユーザは、公認キー（EK）がある場合もない場合も、このファームウェア アップグレード ツールを使用して、ファームウェアをアップグレードできます。 EK がない場合は、ファームウェア アップグレードの実行に権限は必要ありません EK がある場合は、アップグレードに所有者の権限が必要なため、TPM 所有者が存在する必要があります。アップグレードが正常に行われた後、プラットフォームを再起動して、新しいファームウェアを有効にする必要があります BIOS TPM が工場出荷時の状態にリセットされると、所有権は削除され、Embedded Security ソフトウェアのプラットフォームとユーザの初期化のためのウィザードの設定が完了するまで、アップデート機能を使用できません **注記：** ファームウェアのアップデートを実行した後は、必ず再起動してください。 ファームウェア バージョンは、再起動が完了するまで正しく識別されません	1. Embedded Security ソフトウェアを再インストールします 2. [Platform and User Configuration Wizard]（プラットフォームおよびユーザ設定ウィザード）を実行します 3. 以下の手順に従って、システムに Microsoft .NET Framework 1.1 がインストールされていることを確認します a. **[スタート]**をクリックします b. **[コントロール パネル]**をクリックします c. **[プログラムの追加と削除]**をクリックします d. **[Microsoft .NET Framework 1.1]**が表示されていることを確認します 4. 以下の手順に従って、ハードウェアとソフトウェアの構成を確認します a. **[スタート]**をクリックします b. **[すべてのプログラム]**をクリックします c. **[HP ProtectTools セキュリティ マネージャ]**をクリックします d. ツリー メニューから**[Embedded Security]**を選択します e. **[More Details]**（詳細）をクリックします。システムは、次のような構成になっている必要があります ● Product version（製品バージョン）= V4.0.1 ● Embedded Security State（内蔵セキュリティの状態）: Chip State（チップの状態） = Enabled（有効）、Owner State（所有者の状態） = Initialized（初期化済み）、User State（ユーザの状態） = Initialized（初期化済み）

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
		● Component Info（コンポーネント情報）：TCG Spec. Version（TCG 仕様バージョン）= 1.2 ● Vendor（ベンダ） = Broadcom Corporation ● FW Version（FW バージョン）= 2.18（または、それ以上） ● TPM デバイス ドライバ ライブラリ バージョン 2.0.0.9（またはそれ以上） 5. ファームウェア バージョンが 2.18 でない場合は、TPM ファームウェアをダウンロードしてアップデートします。 TPM ファームウェアの SoftPaq は、HP の Web サイト http://www.hp.com/jp/からダウンロードできます
HP ProtectTools セキュリティ マネージャ：セキュリティ マネージャ インタフェースを閉じたとき、エラーが返されることがある	すべてのプラグイン アプリケーションのロードが終了する前に、セキュリティ マネージャを閉じようとして画面右上の閉じるボタンを使用すると、エラーが発生することがあります（12 回に 1 回ぐらいの割合）	これは、セキュリティ マネージャを終了および再起動するときに、そのタイミングがプラグイン サービス ロード時間の影響を受けることに関連しています。 PTHOST.exe は、他のアプリケーション（プラグイン）を収納するシェルであるため、プラグインのロード時間（サービス）の終了能力の影響を受けます。この問題の根本原因は、プラグインのロード終了にかかる時間が経過していないのにシェルが閉じられたことです セキュリティ マネージャがサービス ロード メッセージ（[Security Manager]（セキュリティ マネージャ）ウィンドウの一番上に表示される）をすべて出力し、左の列にすべてのプラグインが一覧表示されるまで待ちます。 エラーを回避するため、プラグインをロードするときは時間を十分にとってください
HP ProtectTools：無制限のアクセスや制御されていない管理権限によってセキュリティ上のリスクが生じる	クライアント コンピュータへのアクセスが無制限の場合、次のような多くのリスクが生じる可能性があります ● PSD の削除 ● ユーザ設定への悪意のある変更 ● セキュリティ ポリシーや機能の無効化	管理者が最善の方法でエンドユーザの権限を制限し、ユーザのアクセスを制限することをおすすめします 不正なユーザに管理権限を与えないでください
BIOS と OS の Embedded Security パスワードが同期していない	新しいパスワードを BIOS Embedded Security パスワードとして確定しない場合、BIOS の Embedded Security パスワードは、f10 BIOS によって元の内蔵セキュリティ パスワードに戻されます	これは仕様です。このパスワードは、OS の基本ユーザ パスワードを変更し、BIOS Embedded Security パスワードの入力画面で認証すれば、再同期されます
BIOS の TPM ブート前認証を有効にした後、1 人のユーザしかシステムにログオンできない	TPM BIOS の PIN は、ユーザ設定を初期化する最初のユーザに関連付けられます。 コンピュータに複数のユーザが存在する場合は、基本的に、最初のユーザが管理者になります。 他のユーザがログオンするには、最初のユーザがそのユーザに自分の TPM ユーザ PIN を通知する必要があります	これは仕様です。ユーザの IT 部門が適切なセキュリティ ポリシーに従ってセキュリティ ソリューションを展開すること、さらに BIOS 管理者パスワードはシステム レベルで保護されるように必ず IT 管理者が設定することをおすすめします

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
TPM を工場出荷時設定に戻した後に TPM ブート前認証を機能させるには、ユーザは自分の PIN を変更する必要がある	設定を戻した後に TPM の BIOS 認証を機能させるには、ユーザは自分の PIN を変更するか、または別のユーザを作成してユーザ設定を初期化する必要があります。 TPM の BIOS 認証を機能させるためのオプションはありません	これは仕様です。工場出荷時設定に戻すと基本ユーザ キーが消去されます。 基本ユーザ キーを再び初期化するには、ユーザは自分のユーザ PIN を変更するか、または新しいユーザを作成する必要があります
Embedded Security の **[Reset to Factory Settings]**（工場出荷時の設定に戻します）を使用しても、**[Power-on authentication support]**（起動時の認証サポート）が初期設定にならない	コンピュータ セットアップ（F10）ユーティリティで、Embedded Security デバイス オプションの**[Reset to Factory Settings]**（工場出荷時の設定に戻します）を使用しても、**[起動時の認証サポート]**オプションは工場出荷時の設定にリセットされません。初期設定では、**[Power-on authentication support]**（起動時の認証サポート）は、**[Disable]**（無効）に設定されます	**[Reset to Factory Settings]**（工場出荷時の設定に戻します）オプションによって内蔵セキュリティ デバイスが無効になり、それによって、他の Embedded Security オプション（**[Power-on authentication support]**（起動時の認証サポート）を含む）が非表示になります。 ただし、内蔵セキュリティ デバイスを再度有効にすると、**[Power-on authentication support]**（起動時の認証サポート）が有効のままになります HP では解決策に向けた取り組みを進めており、将来の Web ベース ROM の SoftPaq で提供する予定です
起動処理中、セキュリティ電源投入時認証が BIOS パスワードと重複している	電源投入時認証では、ユーザは TPM パスワードを使用してシステムにログオンするよう求められますが、**[f10]**キーを押して BIOS にアクセスすると、読み取りのアクセス権のみを許可されます	BIOS への書き込みを可能にするには、電源投入時認証のウィンドウで、TPM パスワードの代わりに BIOS パスワードを入力する必要があります
所有者のパスワードを変更した後、[Computer Setup]を介して BIOS により古いパスワードと新しいパスワードの両方の入力が求められる	Windows の Embedded Security ソフトウェアで所有者のパスワードを変更した後、[Computer Setup]を介して BIOS により古いパスワードと新しいパスワードの両方の入力が求められます	これは仕様です。 オペレーティング システムの起動後に、BIOS が TPM と通信できず、TPM のパスフレーズを確認できないことが原因です

用語集

BIOS セキュリティ モード　有効にすると、ユーザ認証に Java Card および有効な PIN の使用が必要になる、Java Card セキュリティでの設定。

BIOS プロファイル　他のアカウントに保存および適用できる、BIOS 設定値の集合。

DriveLock　ハードドライブをユーザにリンクして、コンピュータの起動時にユーザに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

ID　HP ProtectTools Credential Manager 内で、特定のユーザのアカウントまたはプロファイルのように処理される、証明情報と設定の集合。

Java Card　所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。 所有者をコンピュータに対して認証するために使用されます。

PSD（Personal Secure Drive）　機密情報を保護するための記憶領域を提供する機能。

TPM（Trusted Platform Module）内蔵セキュリティ チップ（一部のモデルのみ）　機密性の高いユーザ情報を悪意のある攻撃者から保護できる、統合されたセキュリティ チップ。 特定のプラットフォーム上の信頼性の基盤です。 TPM によって、TCG（Trusted Computing Group）仕様に適合する暗号化アルゴリズムおよび演算方法が提供されます。

USB トークン　ユーザに関する識別情報が格納されているセキュリティ デバイス。 Java Card や指紋認証システムと同様に、所有者をコンピュータに対して認証するために使用されます。

Windows ユーザ アカウント　ネットワークまたは個別のコンピュータへのログオンを承認された個人のプロファイル。

暗号化サービス プロバイダ（CSP）　明確なインタフェースを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。

暗号化の解除　暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイル システム（EFS）　選択されたフォルダ内のすべてのファイルおよびサブフォルダを暗号化するシステム。

暗号化　権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。 データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。 一般的な暗号化には、データ暗号化規格（DES）や公開キー暗号があります。

暗号法　特定の個人だけが解読できるように、データを暗号化および暗号化解除する手法。

移行　キーおよび証明情報を管理、復元、および転送する作業。

仮想トークン　Java Card やカード リーダーとよく似た働きをするセキュリティ機能。 このトークンは、コンピュータのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。 仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

緊急リカバリ アーカイブ　他のプラットフォームの所有者キーを使用して基本ユーザ キーを再暗号化できる、保護された記憶領域。

厳重なセキュリティ　電源投入時パスワード、管理者パスワード、およびその他の形態の、電源投入時認証に対する保護機能を強化する、BIOS Configuration にあるセキュリティ機能。

公開キー基盤（PKI）　証明情報および暗号化キーを作成、使用、および管理するためのインタフェースを定義する規格。

自動 DriveLock　DriveLock パスワードが生成され、TPM 内蔵セキュリティ チップによって保護されるようにするセキュリティ機能。 起動時にユーザが正しい TPM 基本ユーザ キーのパスワードを入力し、それが TPM 内蔵セキュリティ チップによって認証されると、BIOS によってそのユーザ用のハードドライブのロックが解除されます。

証明書　ユーザが認証プロセスで特定のタスクに対する適格性を証明するための方法。

シングルサインオン　認証情報を格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに Credential Manager を使用してアクセスできるようにする機能。

スマート カード　所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。 所有者をコンピュータに対して認証するために使用されます。

デジタル証明書　デジタル証明書の所有者の身元と、デジタル情報の署名に使用される電子キーのペアとを結びつけることによって、個人または企業の身元を証明する電子的な信用証明書。

デジタル署名　資料の送信者を証明し、署名された後にファイルが変更されていないことを証明するファイルとともに送信されるデータ。

電源投入時認証　Java Card、セキュリティ チップ、パスワードなど、コンピュータの起動時に何らかの形式の認証を要求するセキュリティ機能。

ドメイン　ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピュータの集合。 ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

認証機関　公開キー基盤の運営に必要な証明書を発行するサービス。

認証　ユーザがタスクの実行（たとえば、コンピュータへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

ネットワーク アカウント　ローカル コンピュータ上、ワークグループ内、またはドメイン上の Windows ユーザまたは管理者のアカウント。

バイオメトリック（生体認証）　指紋などの身体的な特徴を使用してユーザを識別する認証証明のカテゴリ。

リブート　コンピュータを再起動するプロセス。

索引